February 2022 Update

Protect Your Devices!

Online Security

Tricks and Tips

Advanced Tutorials & Guides

Expert Pro Tips & Hacks

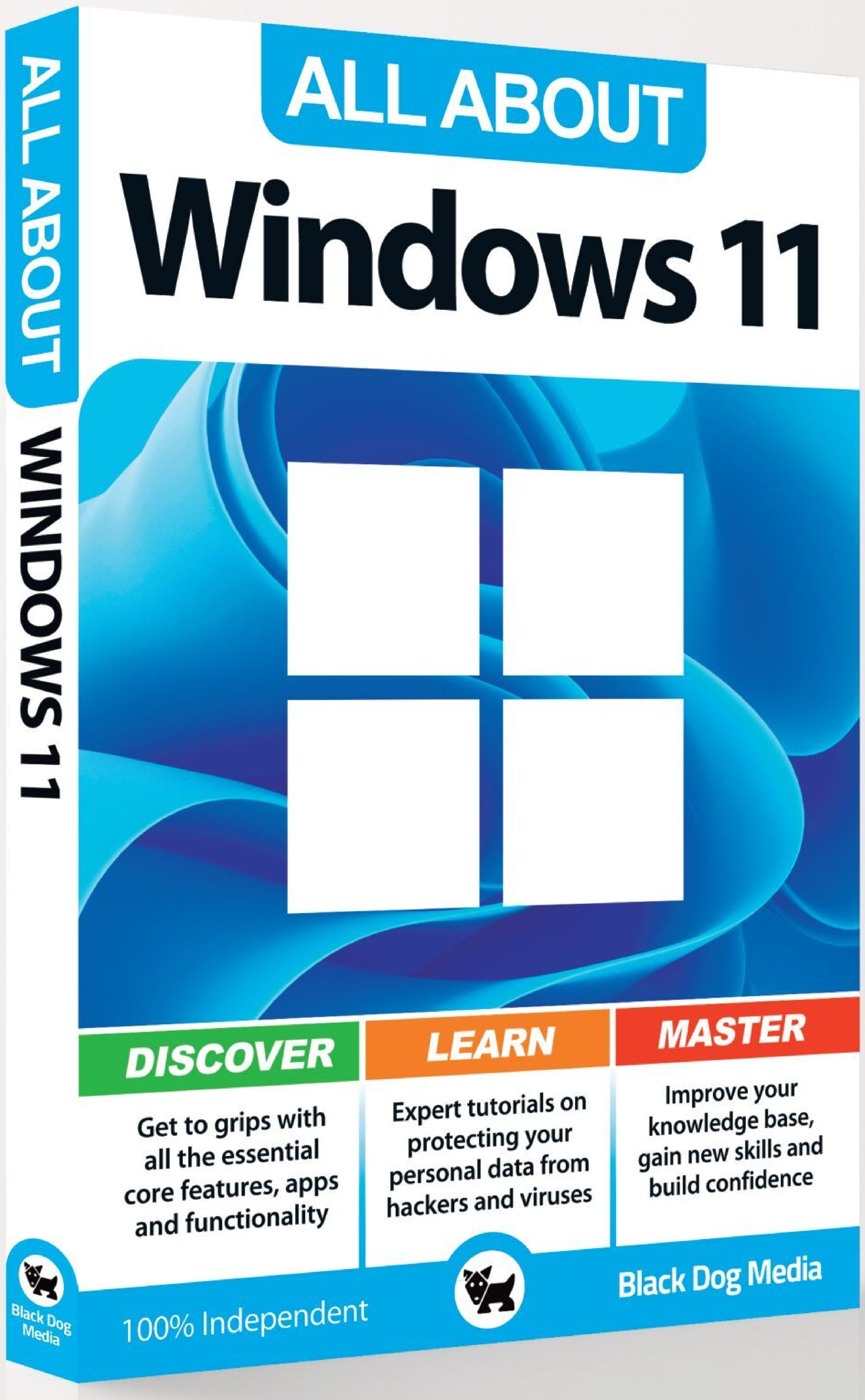
Keep Your Family Safe & Secure

Over 445 Secrets & Hacks

Discover Windows 11.
Learn New Features.
Master Your Desktop.

Black Dog Media

NEW PRINT EDITION


ALL ABOUT
Windows 11
ALL ABOUT WINDOWS 11
DISCOVER
Get to grips with all the essential core features, apps and functionality
LEARN
Expert tutorials on protecting your personal data from hackers and viruses
MASTER
Improve your knowledge base, gain new skills and build confidence
Black Dog Media
100% Independent
Black Dog Media

Over 250 Pages of Expert Tutorials, Guides & Tips!

FEATURED INSIDE:

- Navigating the Start Menu
- Connecting to the Internet
- How to personalise Windows 11
- Web browsing with Edge
- Using OneDrive Cloud Storage
- Video chatting with Skype
- Email, Social Media & Messaging
- Improving Windows 11 security
- Wi-fi and Personal wi-fi hotspots
- Speeding up your computer
- Troubleshooting & User Advice and much more...

Click the link to **BUY NOW** from amazon

https://amzn.to/3EZFHKC

Available in all good bookshops

Online Security

Tricks and Tips

Welcome to the next level of understanding and expansion of your user experience!

For some it is enough to master the basics of your new device, software or hobby. Yet for many, like you, that's just the start! Advancing your skill set is the goal of all users of consumer technology and our team of long term industry experts will help you achieve exactly that. Over this extensive series of titles we will be looking in greater depth at how you make the absolute most from the latest consumer electronics, software, hobbies and trends! We will guide you step-by-step through using all the advanced aspects of the technology that you may have been previously apprehensive at attempting. Let our expert guide help you build your understanding of technology and gain the skills to take you from a confident user to an experienced expert.

Over the page our journey continues, and we will be with you at every stage to advise, inform and ultimately inspire you to go further.

Contents

6 Advanced Security Tips

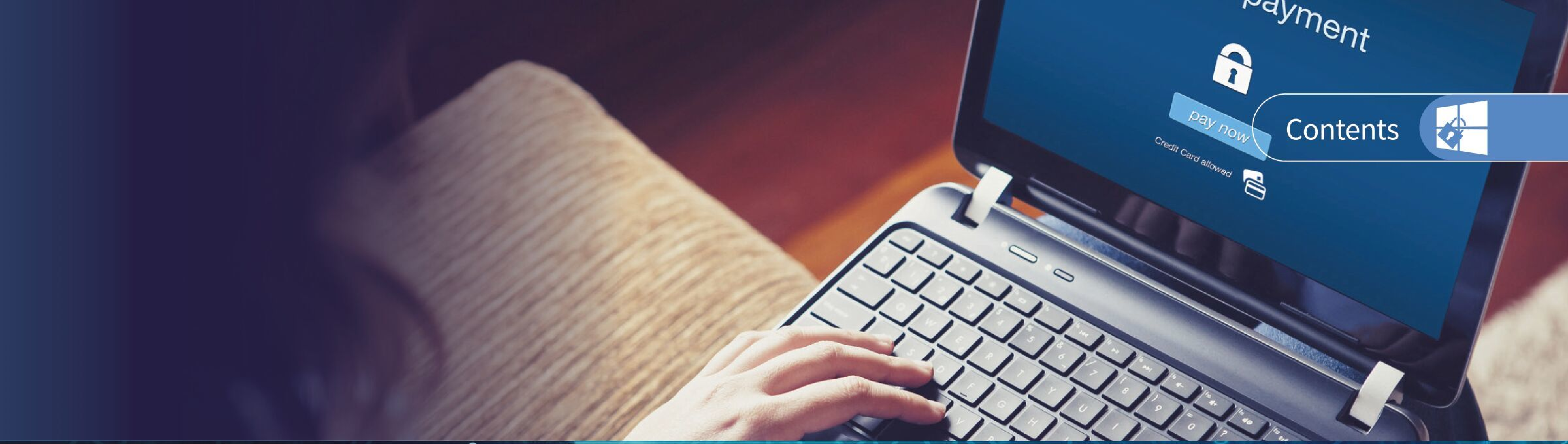
8 Windows 10 Privacy Settings
10 How to Check which Apps are Sending Information
12 What is a firewall?
14 Improving the Windows 10 Firewall
16 Creating a Security Plan
18 Windows Security Checklist
20 What is a Sandbox?
22 Running Windows 10 as a Sandbox
24 Installing VirtualBox
26 Installing Windows 10 in VirtualBox
28 Creating VirtualBox Snapshots of Windows 10
30 Create a Windows 10 Recovery Drive
32 How to Back Up Windows 10
34 How to Create a Windows 10 System Image
36 Extreme Windows 10 Lockdown Tips
38 Cyber and Windows Quiz
40 What the Experts Say

42 Online Child Protection

44 Children Online: What are the Risks?
46 Social Media & Children
48 Search Engine Safety
50 Online Grooming
52 How Safe are the Sites Your Child Can Access?
54 Email and Child Safety
56 Top Child Friendly Email Programs and Services
58 Cyberbullying
60 How to Prevent and Deal with Cyberbullying
62 Helping Your Child Through the Internet
64 Your Child and Online Gaming, is it Safe?
66 Staying Safe when Gaming Online – Advice for Your Child
68 Monitoring What's Going On
70 Monitoring Online Activity for Non-Technical Guardians
72 Tips for Technical Guardians to Monitor a Child's Online Activity
74 Ten Monitoring Tools to Install and Use
76 Using the Windows Hosts File to Block Sites

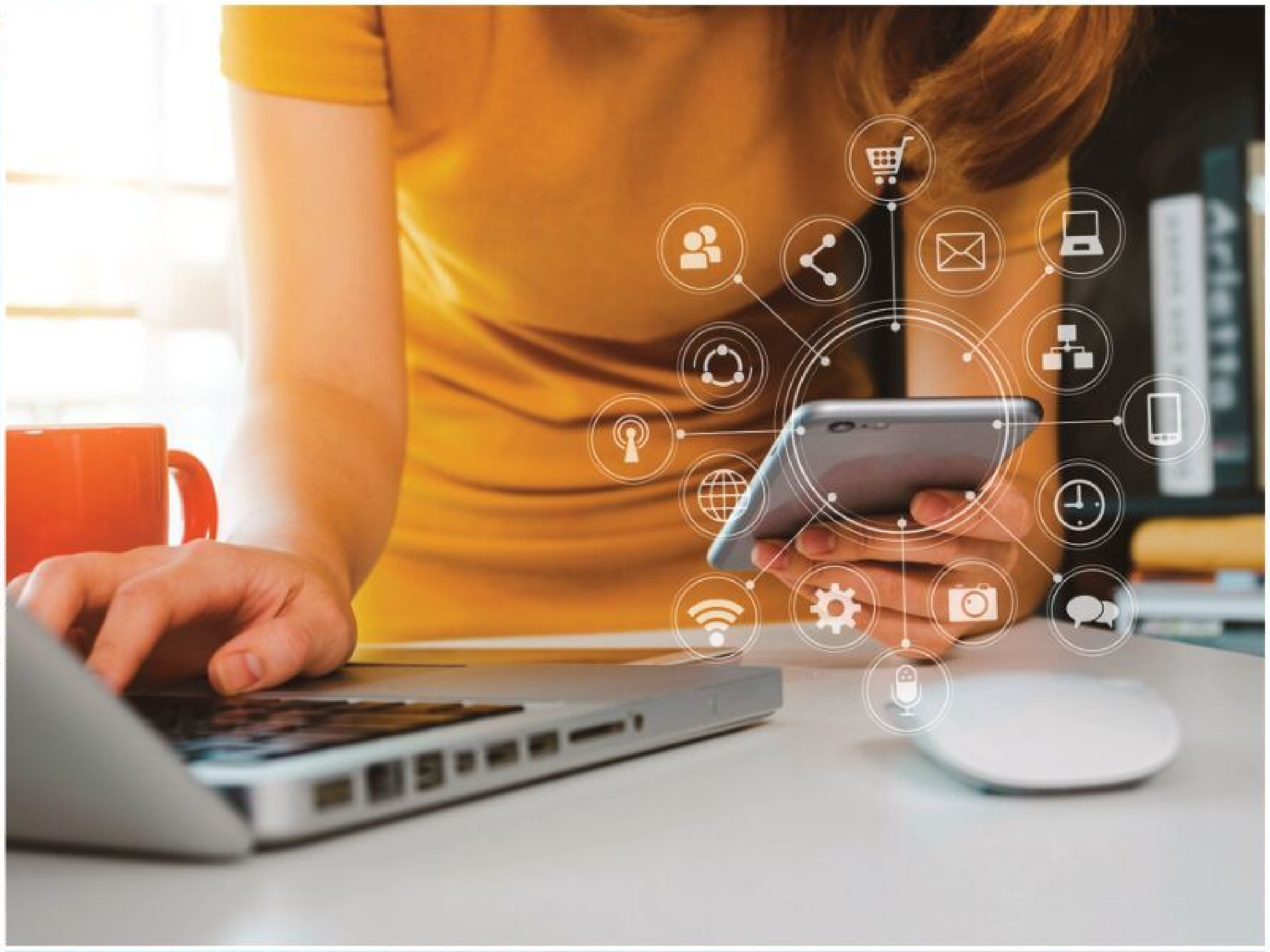
78 Further Protection for Young Adults

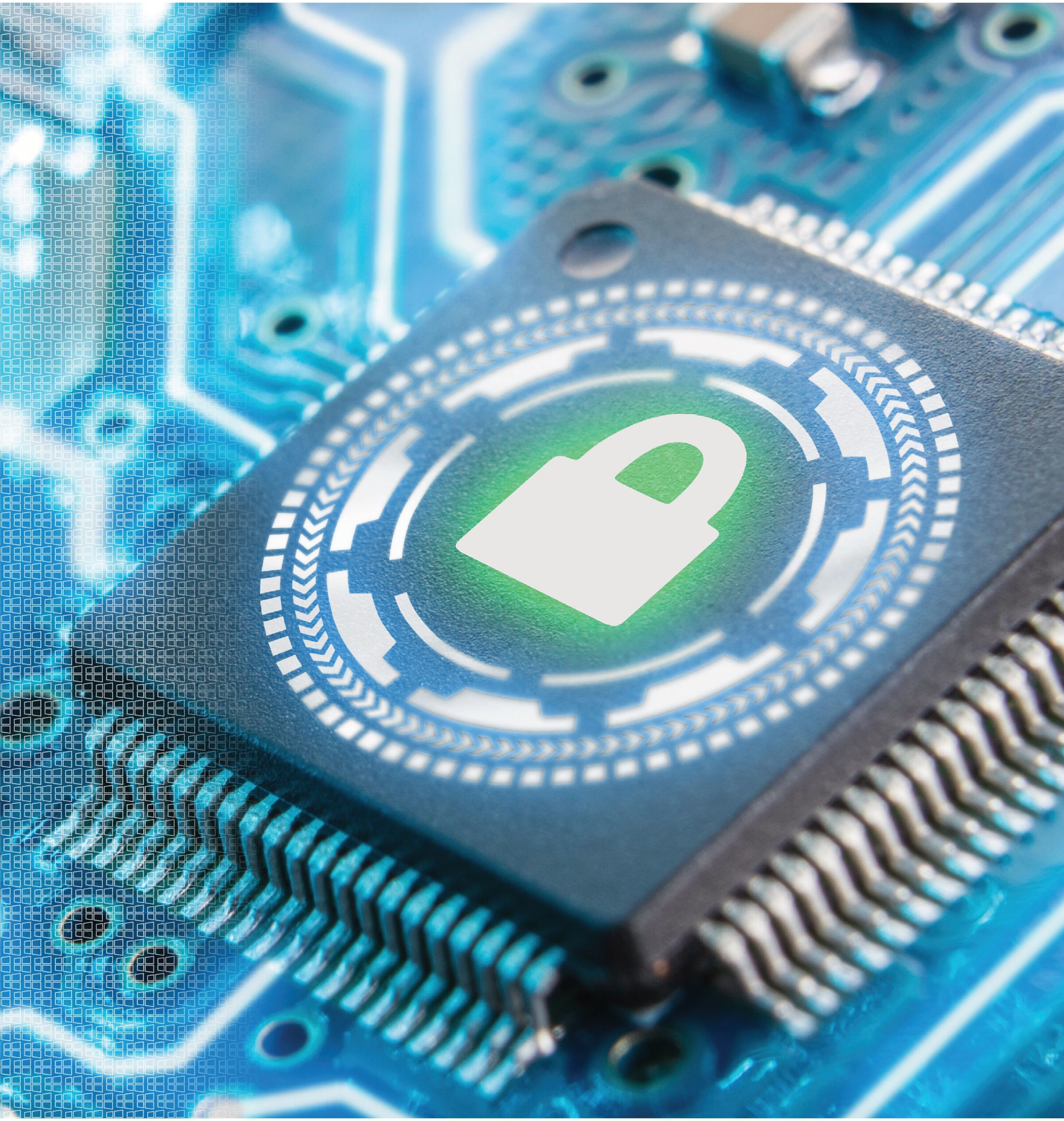
80 Staying Safe with Facebook for Teens
82 Staying Safe with Twitter for Teens
84 Staying Safe with Instagram for Teens
86 Staying Safe with WhatsApp for Teens
88 Staying Safe with Snapchat for Teens
90 Creating a Child Account in Windows 10
92 Windows 10 Family Features
94 Problems with In-app Spending
96 Tips on How to Stop In-app Overspending
98 Online Child Safety at School
100 Where to Find Help with Online Child Safety
102 What the Experts Say
104 Glossary of Terms

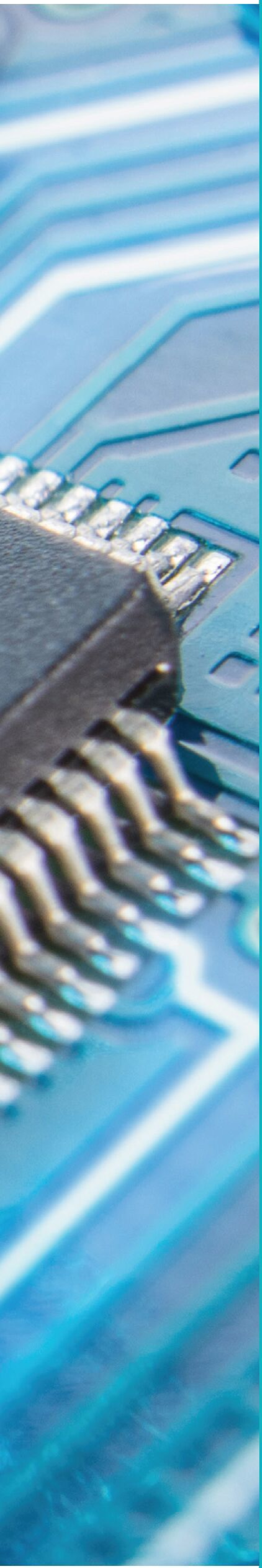


"We live in interesting times, where data is worth more than oil or gold and your personal information is greatly sought after by cybercriminals, scammers and hackers. How prepared are you for this new age of digital vandalism and theft?. For parents and guardians, we also cover looking out for your children when online, together with guides on how best to protect them and advice from industry experts."

Security
ENTER







Advanced Security Tips

If you want to improve your Windows security further, then this section looks at more advanced ways and means in which you can achieve that goal. We cover firewalls, sandboxing and virtual environments and how to tell which programs are communicating beyond your home network.

Our easy to follow tutorials will help you create a reliable backup of Windows 10 and all your data, so should something happen you'll be able to restore your files with confidence.

Windows 10
Privacy Settings

Windows 10's new updates and special edition updates have brought a more customisable degree of control over the operating system's privacy configuration; something that Microsoft has always been criticised for in the past.

Windows 10 is said to be the last true Windows desktop release, with the Redmond company now opting for a rolling release cycle, that will add or remove features over time through regular updates.

> **Going Private**

There are many advantages to this particular setup. A Windows 10 user will always be up to date with regards to security, options and support. Any new hardware that's released will be added to the vast driver database that Windows 10 already uses and it will operate at its maximum potential. Microsoft can gradually roll out features that would require a brand new operating system, thus maximising the capabilities of the OS. Of course, the company can charge for certain additional features that would ordinarily be a part of the OS, such as a media centre for example.

However, profit margins aside, it's the rolling security and updates that the user will benefit greatly from. As Microsoft evolves Windows 10, user and developer feedback can help improve the way the OS protects its user base. A prime example is the new privacy settings available post-Fall Creators Update, which was gradually rolled out to Windows 10 PCs around late October 2017. The privacy settings and options that are now on offer are a radical improvement over the previous, rather bleak, features that came with the original Windows 10 setup. Now, the user has greater control over what the OS can and cannot do to affect an individual's privacy.

Providing you've applied the Fall Creators Update, you can view the current privacy options by clicking the Windows Start button and typing privacy into the search box. Click on the Privacy Settings option, with a padlock icon, and the core privacy options window will open. There are, at the time of writing, nineteen different options available to browse through. Each option, when clicked, will display a subset of available options that can then be enabled or disabled and turned on or off, depending on your preference.

For example the first option, General, offers the user a choice of opting for advertising via apps, allowing websites to provide locally relevant content based on the user's language list and allowing Windows 10 to track how an app is launched to improve search results. Whilst that in itself doesn't sound too much like your privacy is being infiltrated, there are those who don't want the installed apps and the OS having too much knowledge of where they are and what to advertise. Like most privacy options, it's a personal preference as to what you're happy sharing with the system and its connected technologies. Whilst opting to turn every privacy setting on will inevitably open your use of Windows 10 up to whoever or whatever is readily receiving the information, likewise turning everything off will effectively hide you (to some degree); but at the cost of possible loss of available features. There's a fine balance needed to get the best from your privacy and still enjoying Windows 10's many features.

There are some interesting additions to the Fall Creators Update privacy settings, which are certainly worth looking over, if you want a best of both worlds approach to privacy and features.

Location – The Location option will allow Windows 10 and its apps to use your current location to specialise any content. It's innocent enough but for added privacy it's worth considering turning it off.

Camera – This is an excellent addition that will define which installed apps have access to the computer's webcam. You can turn off app access to the camera globally or browse through the apps to decide which has access, or not.

Microphone – The same applies for the computer's microphone; which apps can access it or not, and whether you want to globally turn it off.

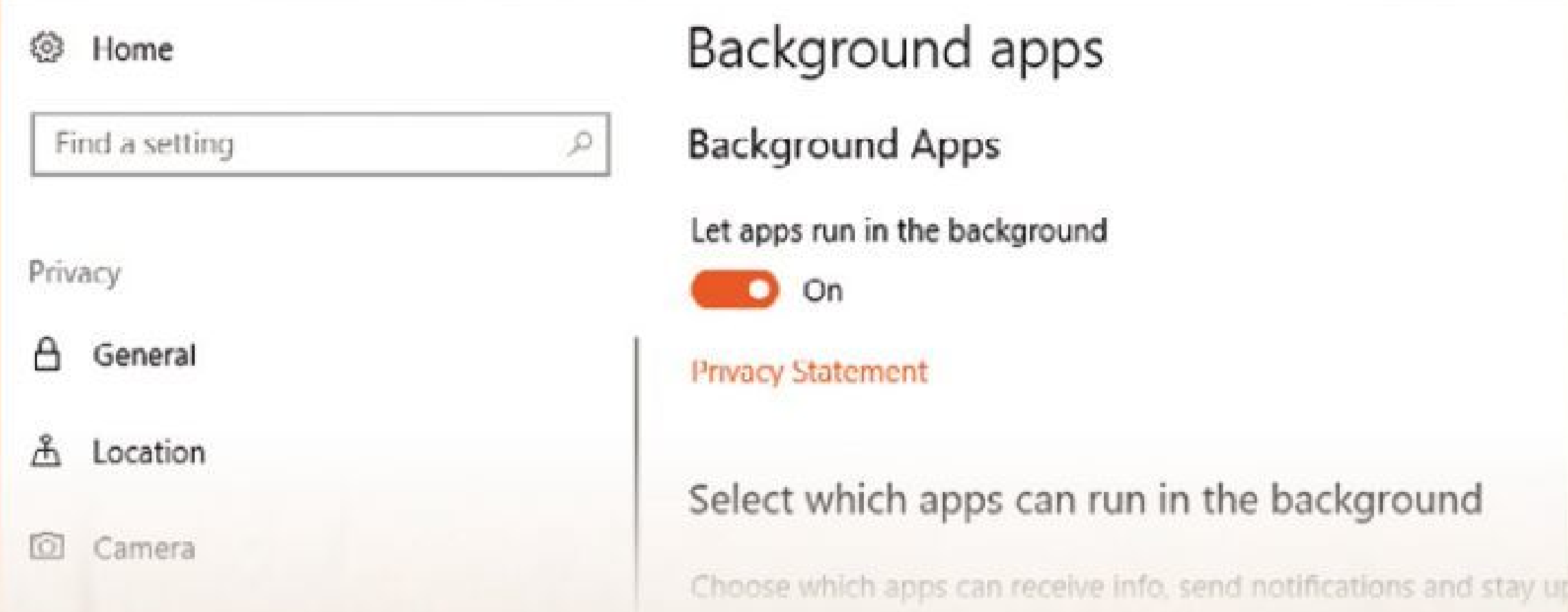
Contacts – The Contacts section details which apps can have access to your current Windows account contacts. Disabling this globally may have a severe impact on how some apps, such as Skype and email work.

Radios – This option will define which apps can control hardware such as the computer's Bluetooth device, Wi-Fi or any other kind of wireless receiver. Obviously, some apps will require access to share information or allow access to shared areas.

Background Apps – Windows 10's background task handling is far better than in previous versions of the operating system. Memory is released as apps drop into the background, as is processor allocation. However, you can further define which apps will be allowed to run in the background with this option.

Taking time to go through each of the available options is something every Windows 10 user should do. This way you become familiar with how the OS shares your account data and what exactly has access to your Windows 10 computer and its hardware.

Which apps are allowed to run silently in the background whilst you work? You can decide whether they do, or not. . .



Background apps

Background Apps

Let apps run in the background

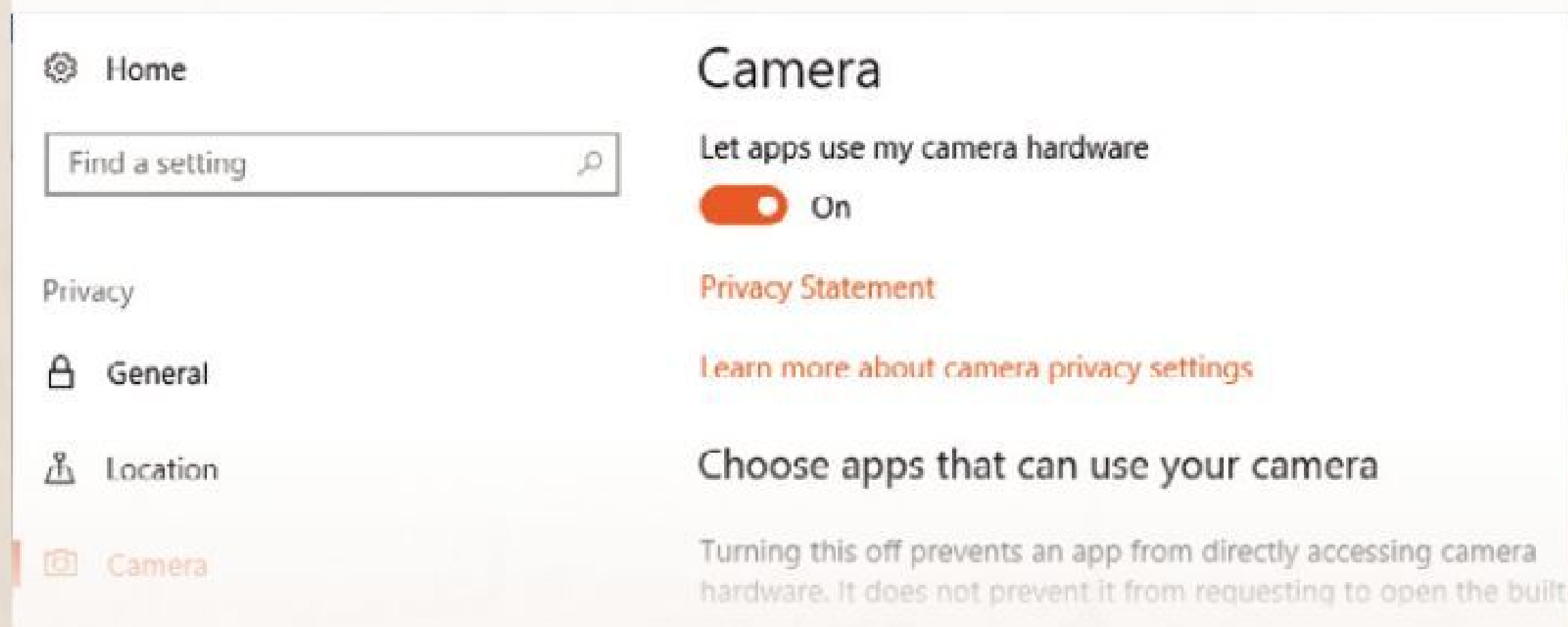
On

Privacy Statement

Select which apps can run in the background

Choose which apps can receive info, send notifications and stay up

You can control which apps have access to the computer's webcam. Handy for keeping track of your privacy. . .



Camera

Let apps use my camera hardware

On

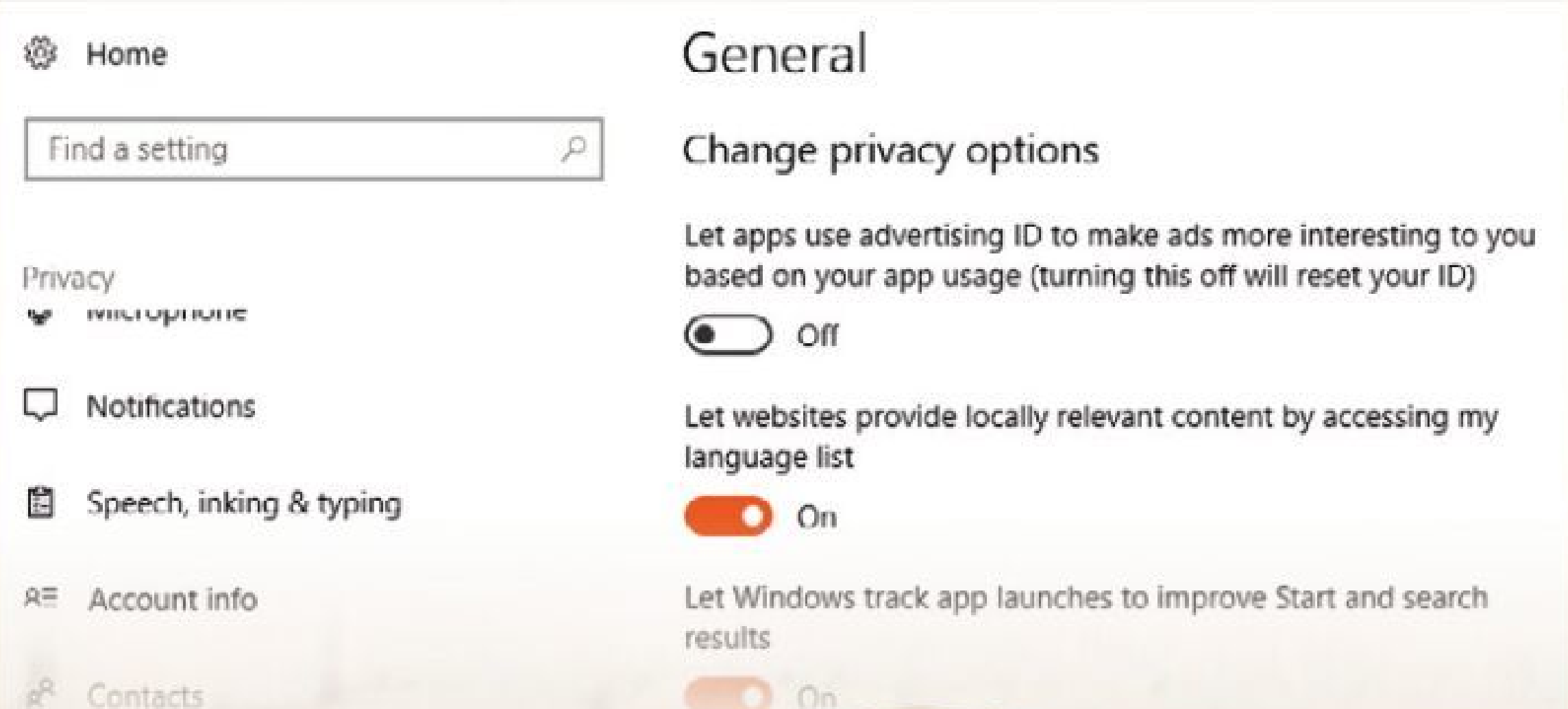
Privacy Statement

Learn more about camera privacy settings

Choose apps that can use your camera

Turning this off prevents an app from directly accessing camera hardware. It does not prevent it from requesting to open the built-

Click the Windows Start button and type privacy, click on the Privacy Settings link and you see this screen . . .



General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)

Off

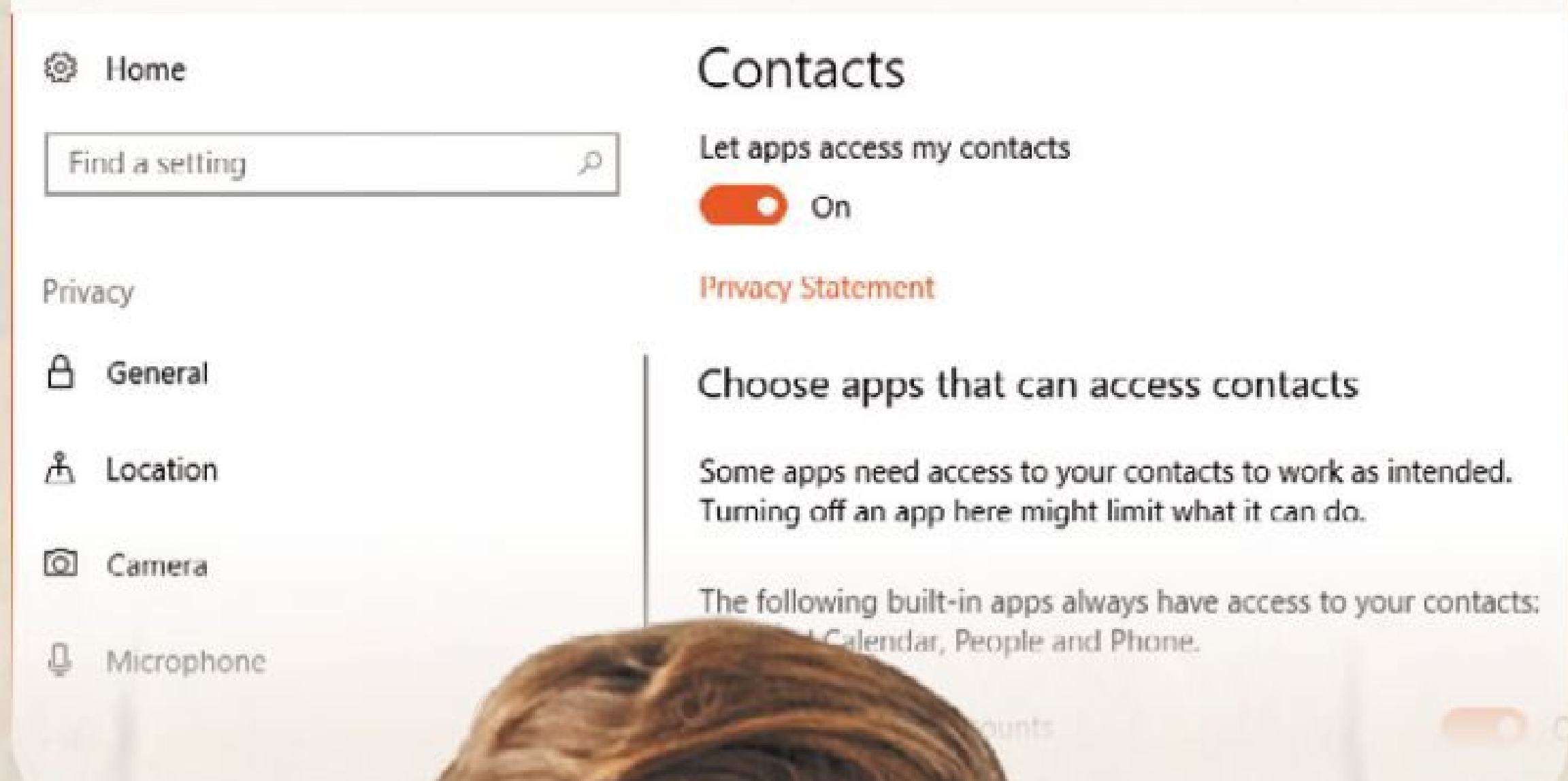
Let websites provide locally relevant content by accessing my language list

On

Let Windows track app launches to improve Start and search results

On

Windows 10's apps can access almost every element of your account, including your contacts. . .



Contacts

Let apps access my contacts

On

Privacy Statement

Choose apps that can access contacts

Some apps need access to your contacts to work as intended. Turning off an app here might limit what it can do.

The following built-in apps always have access to your contacts: Calendar, People and Phone.

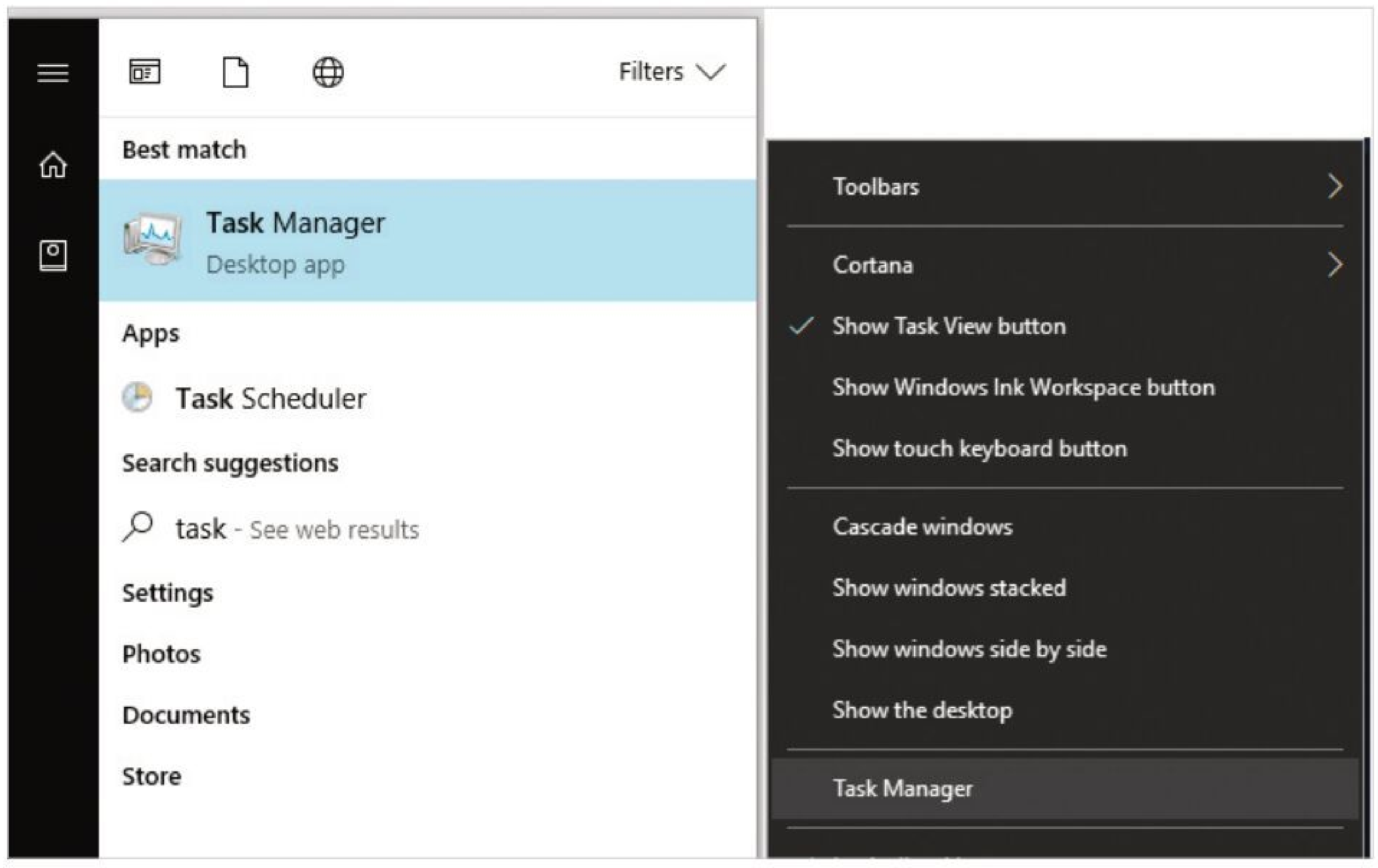
How to Check which Apps are Sending Information

Most Windows 10 apps and programs have some element of code that will attempt to communicate with an external source. That communication could be to check for the latest version, or patches and updates, or it could be malicious software sending personal data.

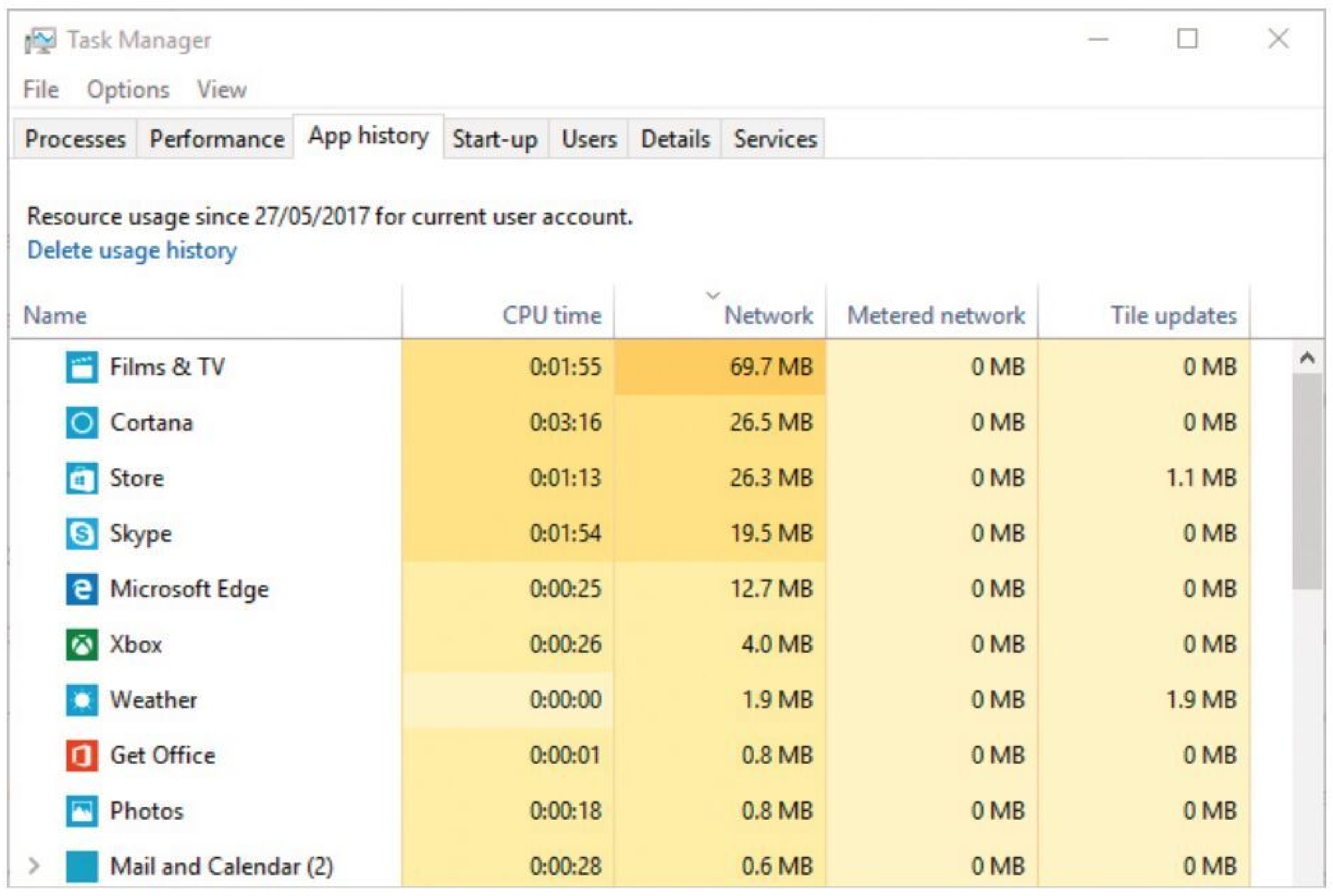
Look Who's Talking

There are a number of ways in which you're able to view which programs and apps are sending data to Internet and external sources. Some methods are better than others, so it's worth trying them all to see which works best for you.

STEP 1 The first port of call to help monitor what apps are accessing the Internet is Task Manager. Click the Windows Start button and type task, then click the Task Manager result in the search box. You can also right-click the taskbar and select Task Manager from the available option in the menu.


Filters
Best match
Task Manager
Desktop app
Apps
Task Scheduler
Search suggestions
task - See web results
Settings
Photos
Documents
Store
Toolbars
Cortana
Show Task View button
Show Windows Ink Workspace button
Show touch keyboard button
Cascade windows
Show windows stacked
Show windows side by side
Show the desktop
Task Manager

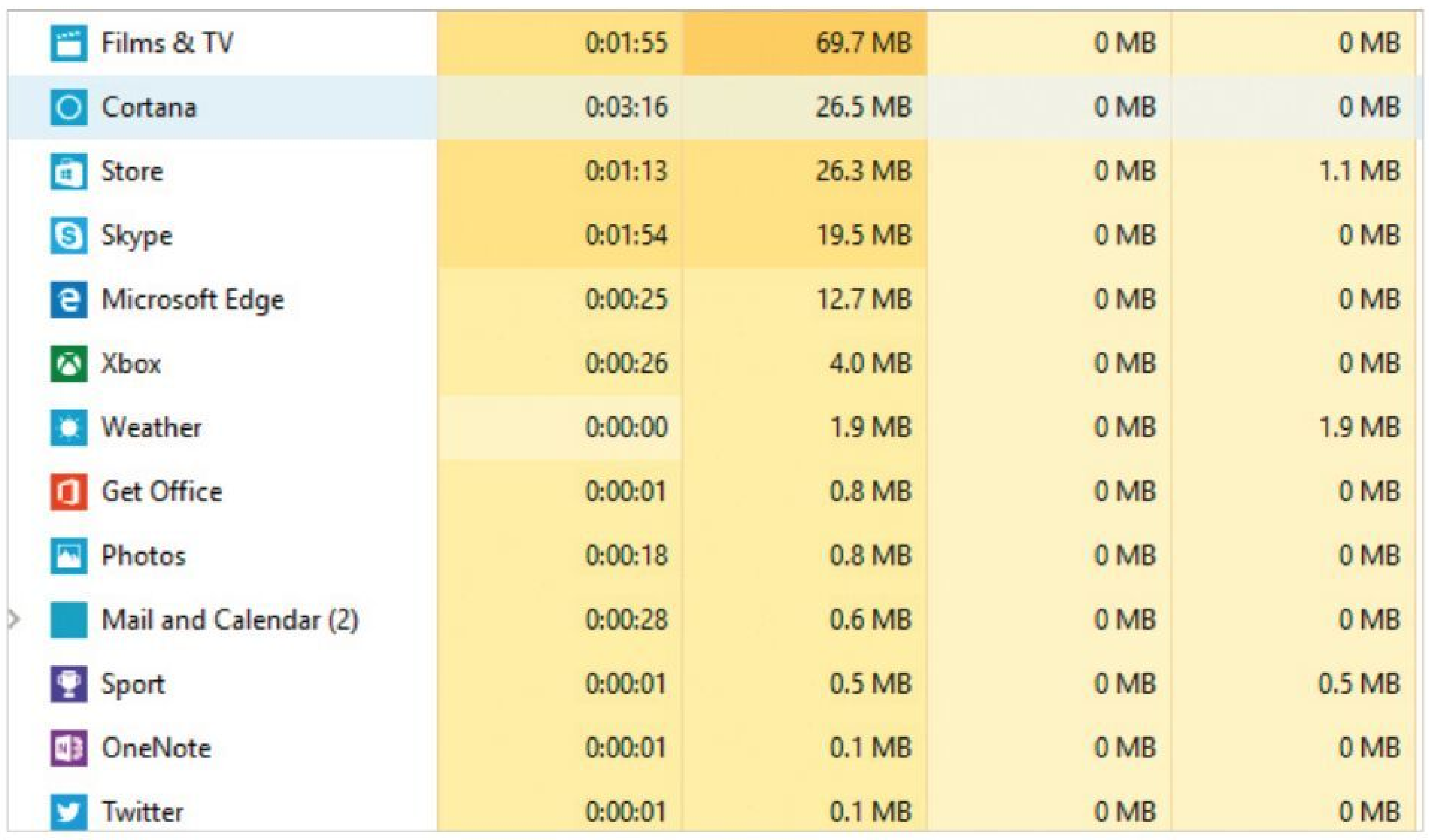
STEP 2 With Task Manager displayed, click the More Details arrow (if it's available). This will expand the Task Manager options. From here, click the App History tab and then the Network column so that there's a downward pointing arrow above it. This indicates network use in a descending order of amount of data sent.


Task Manager
File Options View
Processes Performance App history Start-up Users Details Services

Resource usage since 27/05/2017 for current user account.
Delete usage history

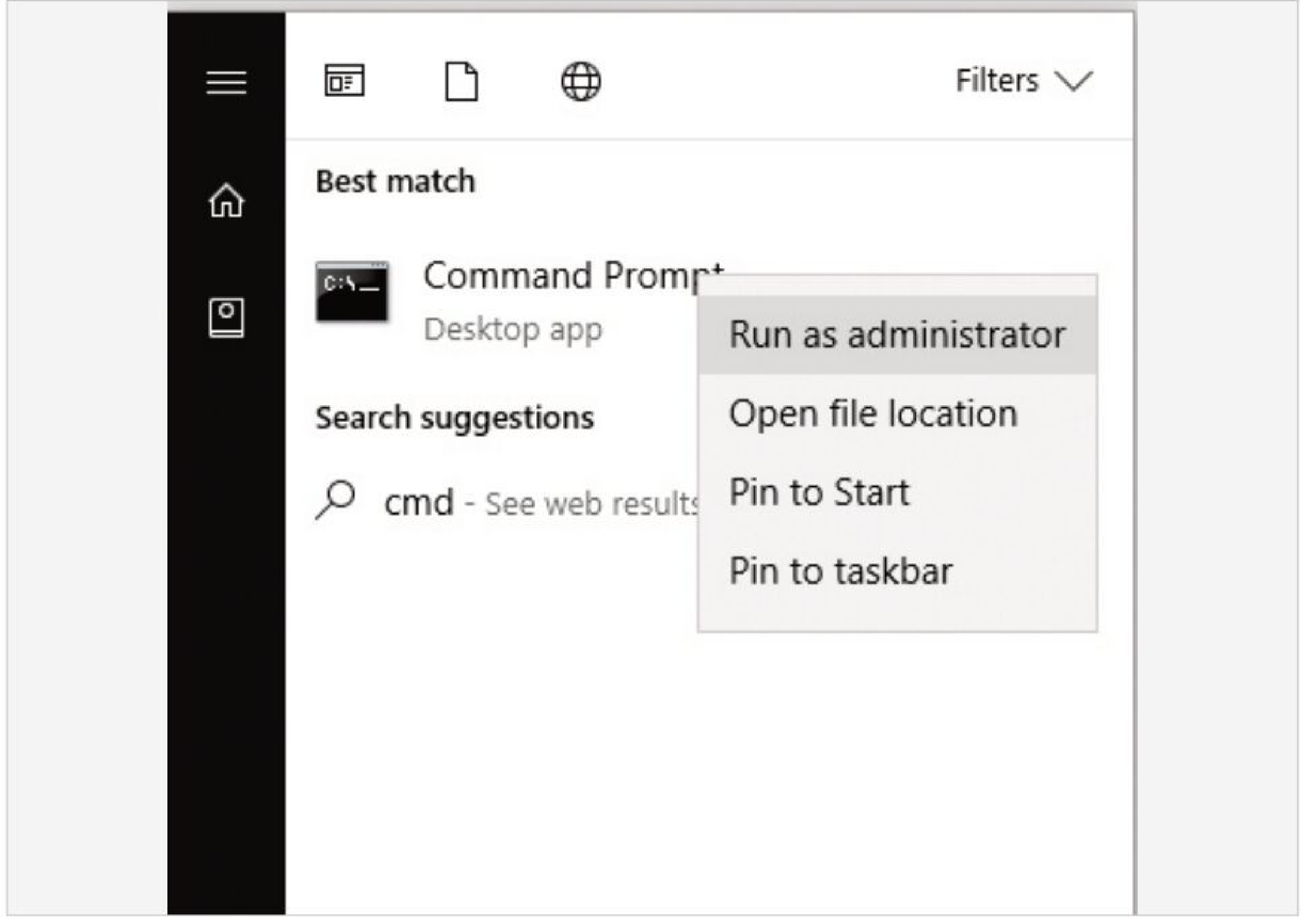
Name	CPU time	Network	Metered network	Tile updates
Films & TV	0:01:55	69.7 MB	0 MB	0 MB
Cortana	0:03:16	26.5 MB	0 MB	0 MB
Store	0:01:13	26.3 MB	0 MB	1.1 MB
Skype	0:01:54	19.5 MB	0 MB	0 MB
Microsoft Edge	0:00:25	12.7 MB	0 MB	0 MB
Xbox	0:00:26	4.0 MB	0 MB	0 MB
Weather	0:00:00	1.9 MB	0 MB	1.9 MB
Get Office	0:00:01	0.8 MB	0 MB	0 MB
Photos	0:00:18	0.8 MB	0 MB	0 MB
Mail and Calendar (2)	0:00:28	0.6 MB	0 MB	0 MB

STEP 3 This is a reasonably accurate way of viewing which installed programs have been accessing the outside world. The amount of data being sent to and from your PC can be quite illuminating, and surprising, as you may never even realise you have a particular app installed never mind that it's communicating with an external source.

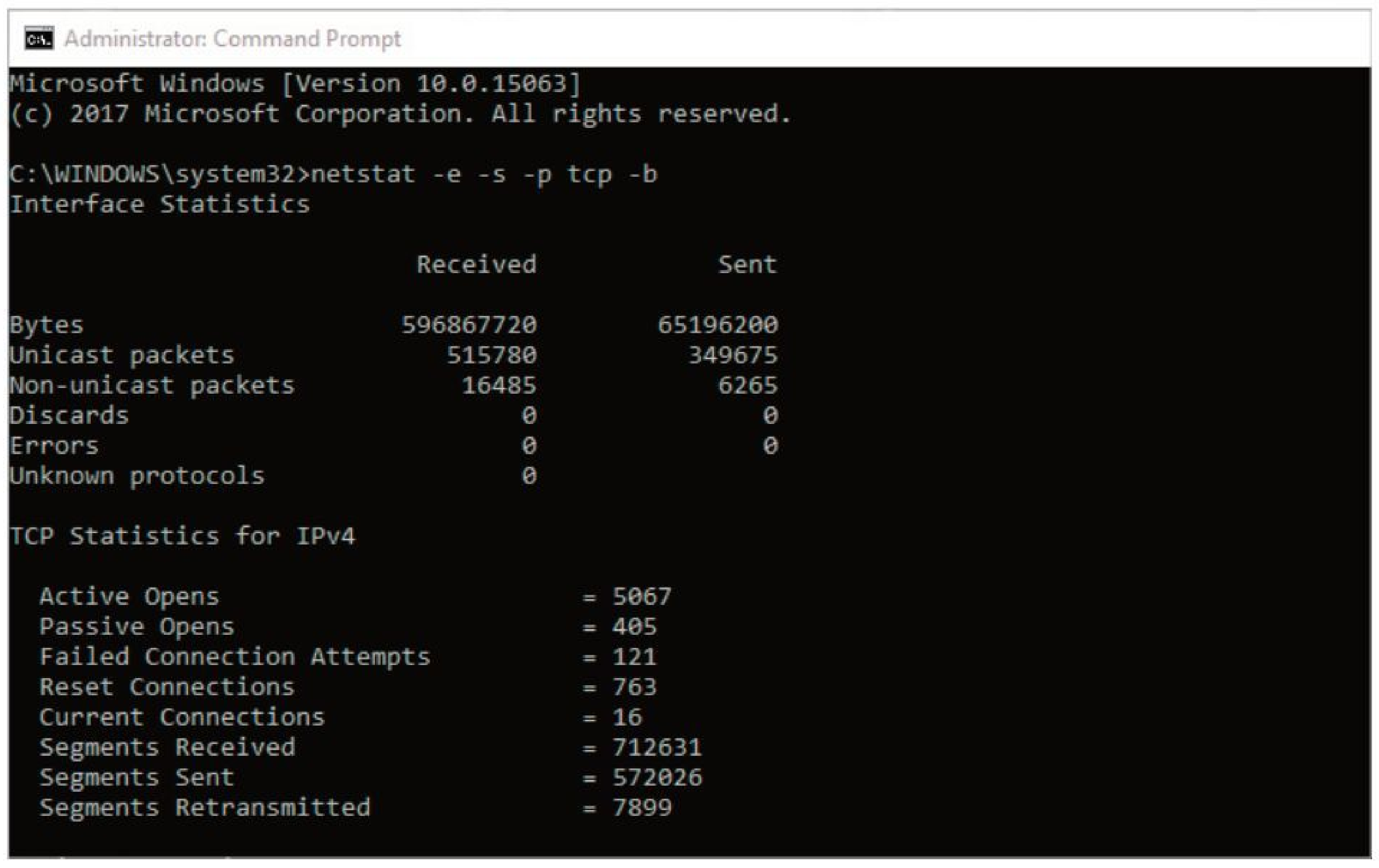


Films & TV	0:01:55	69.7 MB	0 MB	0 MB
Cortana	0:03:16	26.5 MB	0 MB	0 MB
Store	0:01:13	26.3 MB	0 MB	1.1 MB
Skype	0:01:54	19.5 MB	0 MB	0 MB
Microsoft Edge	0:00:25	12.7 MB	0 MB	0 MB
Xbox	0:00:26	4.0 MB	0 MB	0 MB
Weather	0:00:00	1.9 MB	0 MB	1.9 MB
Get Office	0:00:01	0.8 MB	0 MB	0 MB
Photos	0:00:18	0.8 MB	0 MB	0 MB
Mail and Calendar (2)	0:00:28	0.6 MB	0 MB	0 MB
Sport	0:00:01	0.5 MB	0 MB	0.5 MB
OneNote	0:00:01	0.1 MB	0 MB	0 MB
Twitter	0:00:01	0.1 MB	0 MB	0 MB

STEP 4 Another excellent method is by using the Netstat command. Click on the Windows Start button and enter **cmd**, then right-click the Command Prompt option and choose Run as Administrator from the menu. When the message to authenticate the action pops up, click on Yes.

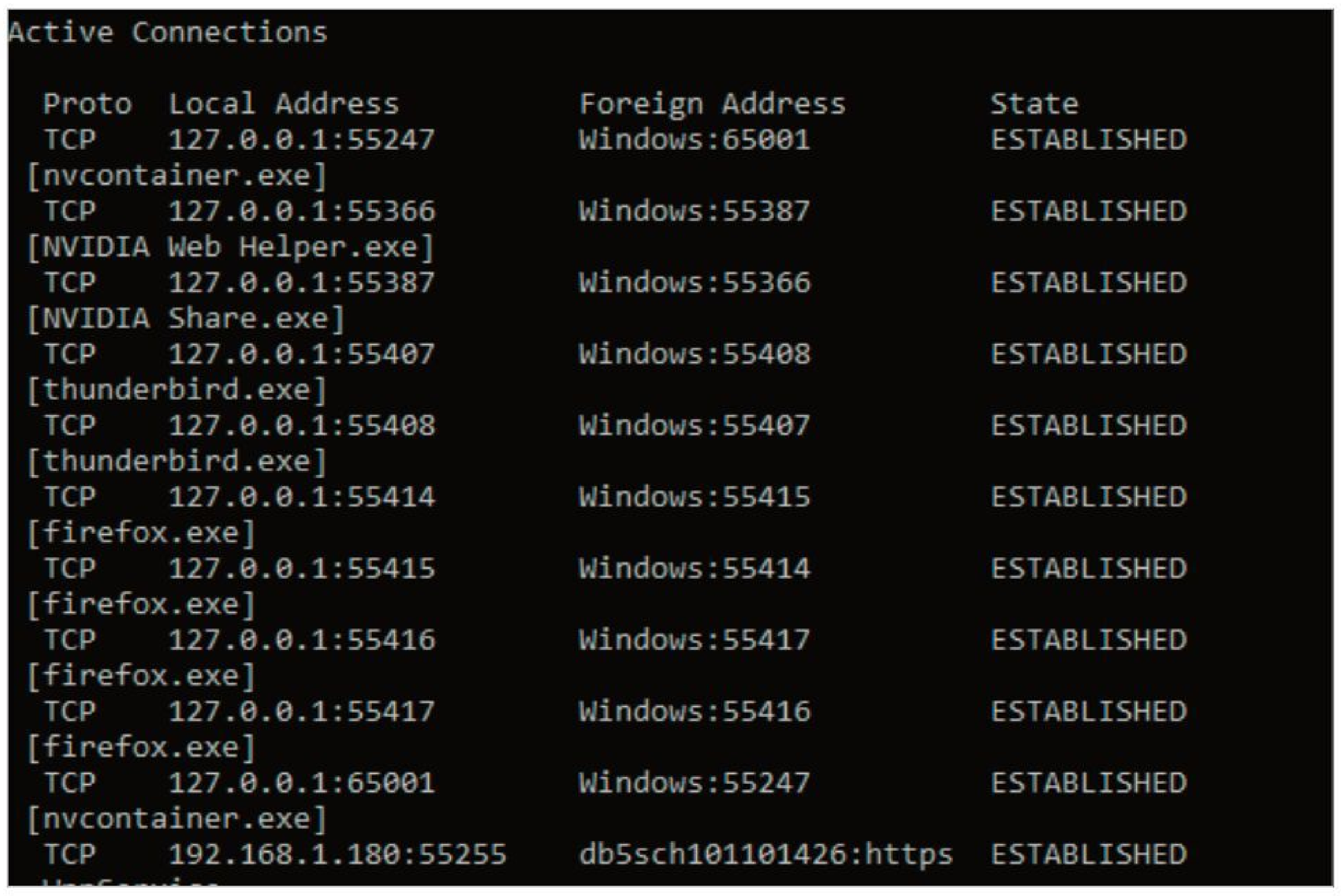

Filters
Best match
Command Prompt
Desktop app
Search suggestions
cmd - See web results
Run as administrator
Open file location
Pin to Start
Pin to taskbar

STEP 5 With the command prompt open enter the following: **netstat -e -s -p tcp -b**. The information populates the command prompt box quickly, so you need to scroll back up to the top to see it in its entirety.



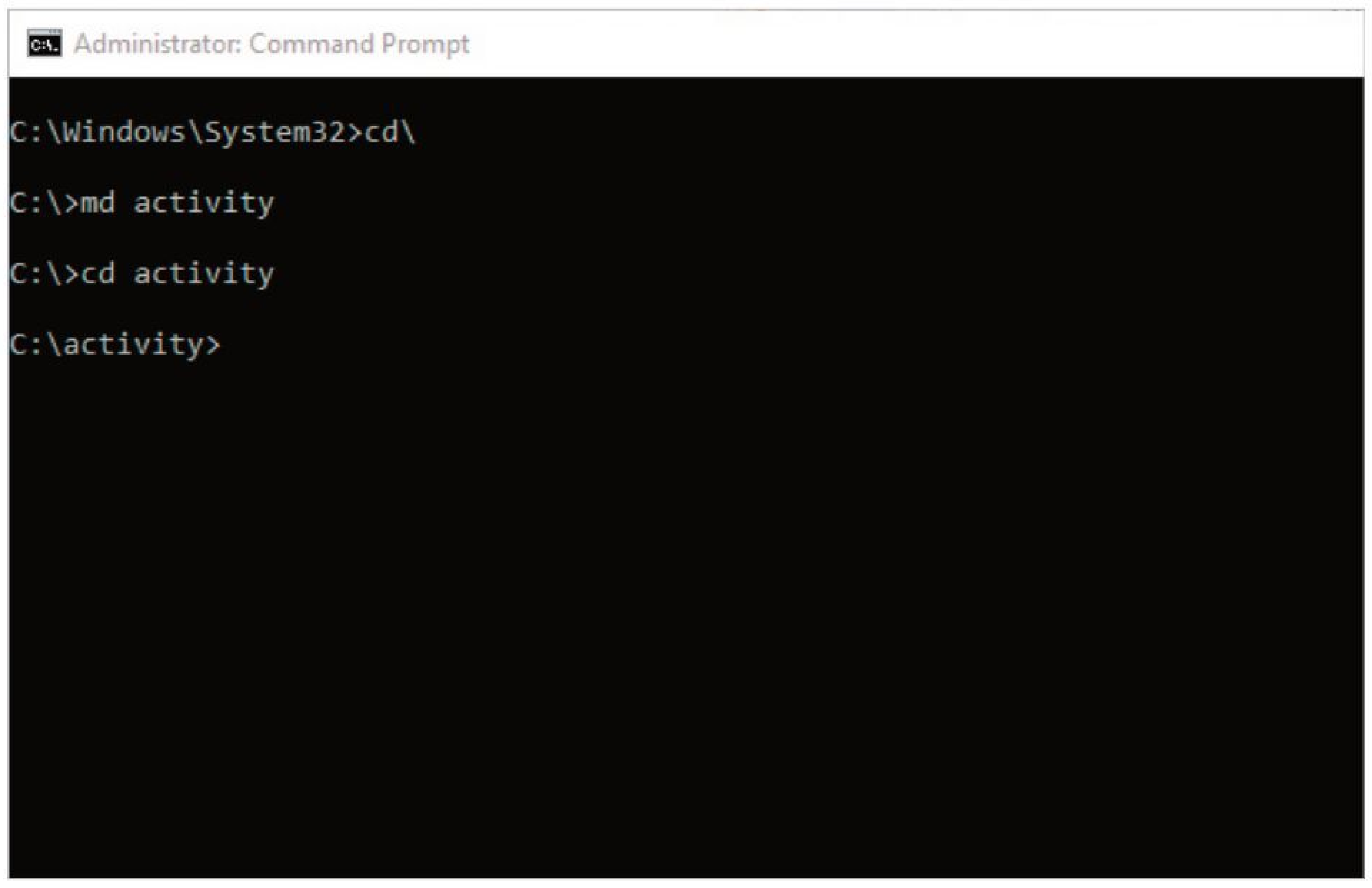
```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -e -s -p tcp -b
Interface Statistics

                           Received            Sent

Bytes                     596867720        65196200
Unicast packets              515780          349675
Non-unicast packets           16485            6265
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

TCP Statistics for IPv4

  Active Opens                        = 5067
  Passive Opens                       = 405
  Failed Connection Attempts          = 121
  Reset Connections                   = 763
  Current Connections                 = 16
  Segments Received                   = 712631
  Segments Sent                       = 572026
  Segments Retransmitted              = 7899
```

STEP 6 What you're looking at here is a list of programs, from the column to the far left, with the IP address of its source and the destination address in the middle column; with a third column detailing if the connection is established or not. It can be confusing to view at first but after a moment or two it should begin to make sense.



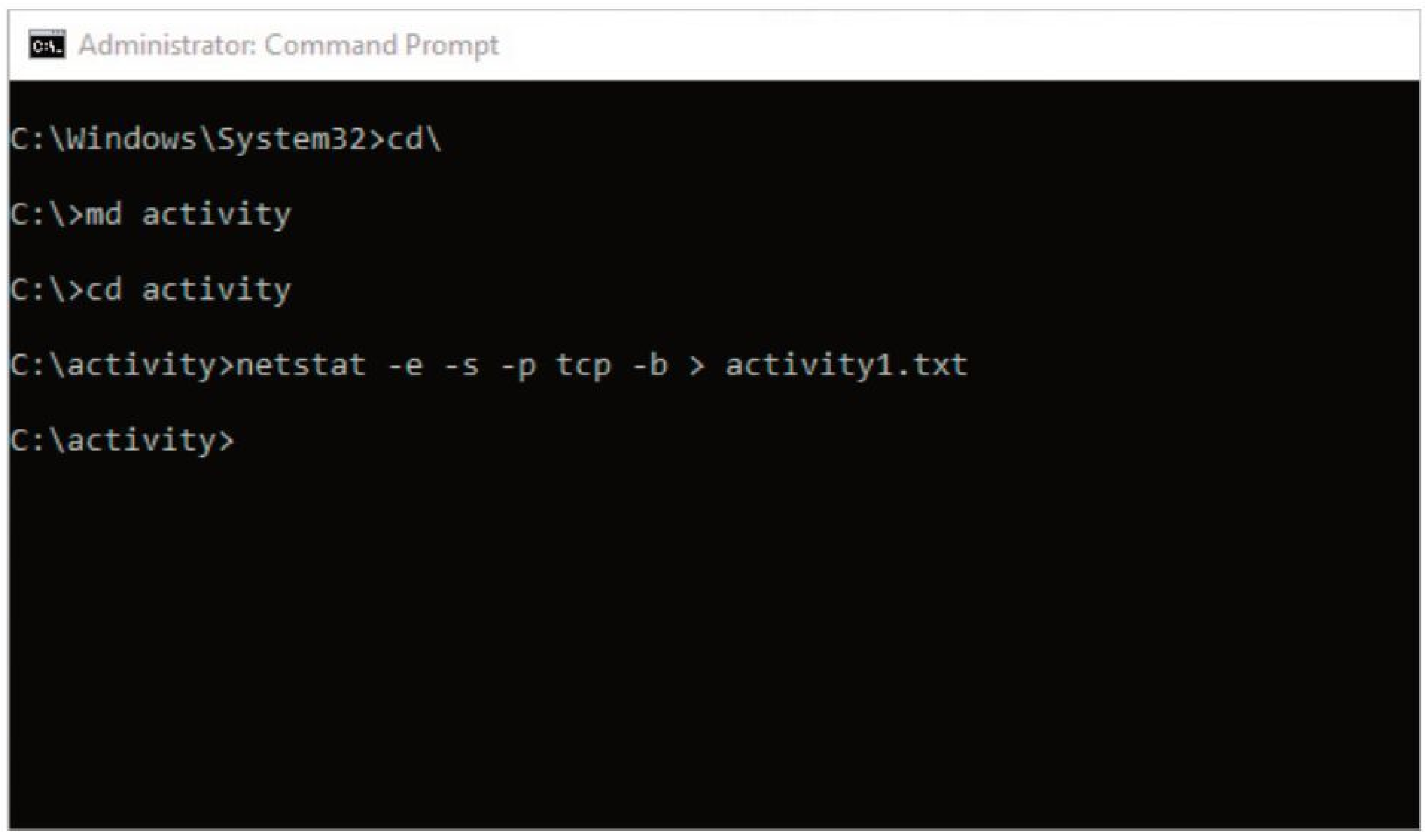
```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:55247        Windows:65001          ESTABLISHED
 [nvcontainer.exe]
  TCP    127.0.0.1:55366        Windows:55387          ESTABLISHED
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:55387        Windows:55366          ESTABLISHED
 [NVIDIA Share.exe]
  TCP    127.0.0.1:55407        Windows:55408          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55408        Windows:55407          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55414        Windows:55415          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55415        Windows:55414          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55416        Windows:55417          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55417        Windows:55416          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:65001        Windows:55247          ESTABLISHED
 [nvcontainer.exe]
  TCP    192.168.1.180:55255    db5sch101101426:https  ESTABLISHED
```

STEP 7 If you want to create a friendlier way of viewing Netstat active connection data, you can pipe the contents to a text file. For example, in the command prompt enter **cd** to take you to the root of the C: drive. Then create a new folder to store the text file with **md activity**, and enter it with **cd activity**.



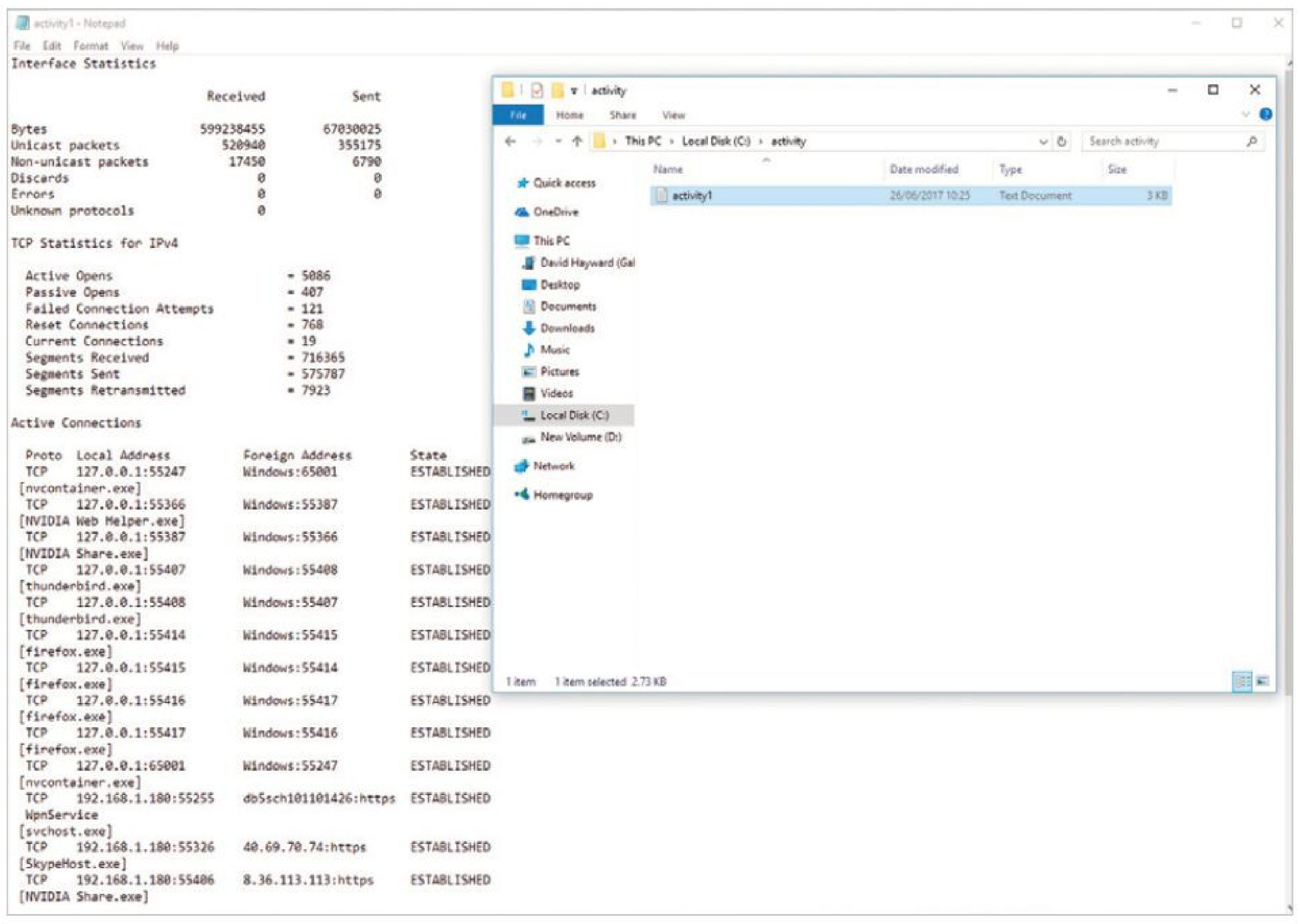
```
C:\Windows\System32>cd\

C:\>md activity

C:\>cd activity

C:\activity>
```

STEP 8 In the activity folder, enter the following: **netstat -e -s -p tcp -b > activity1.txt**. This is the same command as before but this time the output is being sent to a text file, named activity1.txt, rather than outputting to the command prompt window.



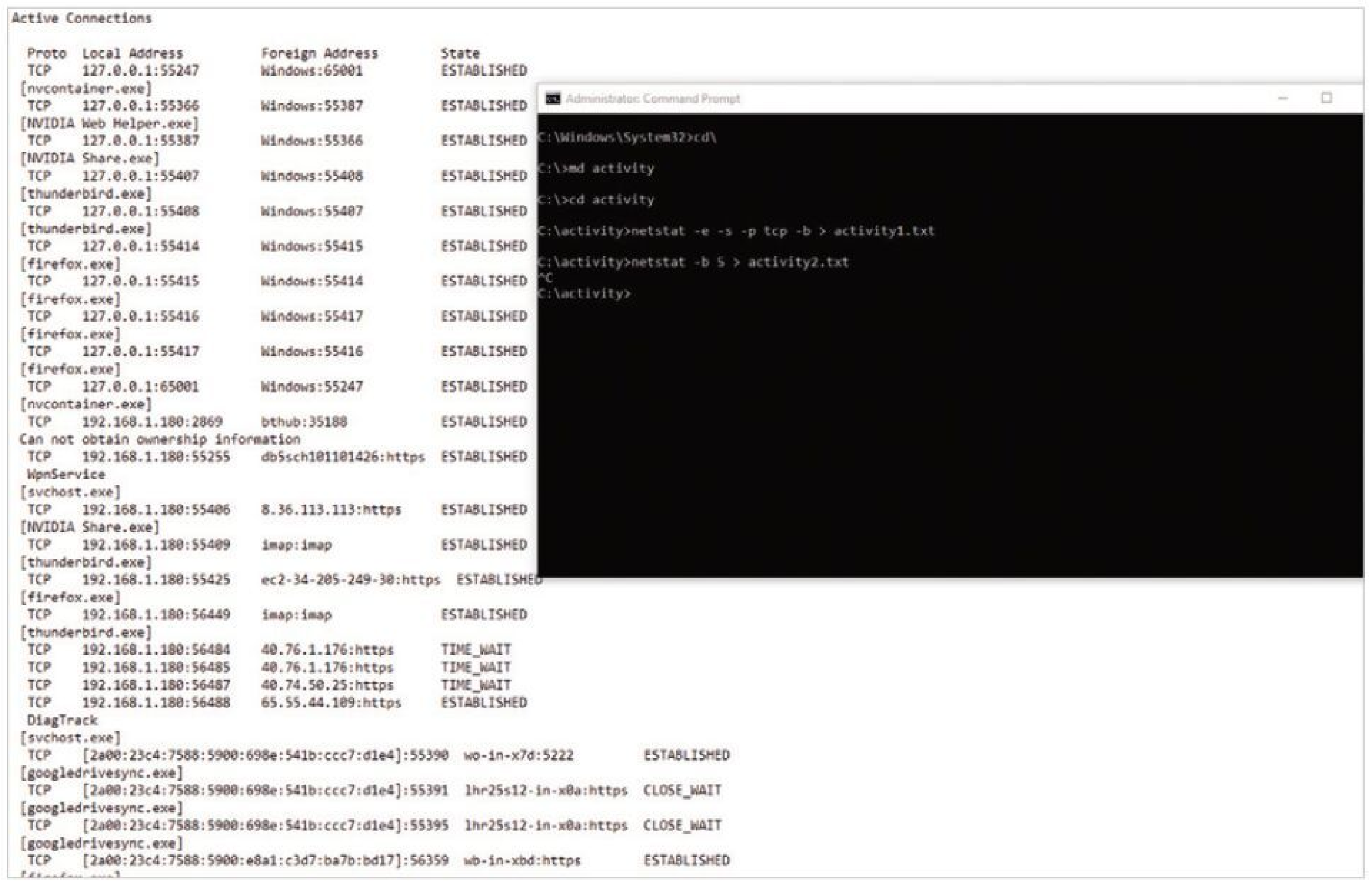
```
C:\Windows\System32>cd\

C:\>md activity

C:\>cd activity

C:\activity>netstat -e -s -p tcp -b > activity1.txt

C:\activity>
```

STEP 9 Using Windows Explorer, locate the C:\activity folder you created and within the activity1.txt file. Double-click the **activity1.txt** file and it opens in Notepad where you're able to view it without the often difficult to read command prompt window.



```
Interface Statistics

                           Received            Sent

Bytes                     599238455        67030025
Unicast packets              520940          355175
Non-unicast packets           17450            6790
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

TCP Statistics for IPv4

  Active Opens                        = 5086
  Passive Opens                       = 407
  Failed Connection Attempts          = 121
  Reset Connections                   = 768
  Current Connections                 = 19
  Segments Received                   = 716365
  Segments Sent                       = 575787
  Segments Retransmitted              = 7923

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:55247        Windows:65001          ESTABLISHED
 [nvcontainer.exe]
  TCP    127.0.0.1:55366        Windows:55387          ESTABLISHED
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:55387        Windows:55366          ESTABLISHED
 [NVIDIA Share.exe]
  TCP    127.0.0.1:55407        Windows:55408          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55408        Windows:55407          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55414        Windows:55415          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55415        Windows:55414          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55416        Windows:55417          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55417        Windows:55416          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:65001        Windows:55247          ESTABLISHED
 [nvcontainer.exe]
  TCP    192.168.1.180:55255    db5sch101101426:https  ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    192.168.1.180:55326    40.69.70.74:https      ESTABLISHED
 [SkypeHost.exe]
  TCP    192.168.1.180:55406    8.36.113.113:https     ESTABLISHED
 [NVIDIA Share.exe]
```

STEP 10 If you want to simplify the information and the process, enter: **netstat -b 5 > activity2.txt** into the command prompt within the activity folder on the C: drive. This will record the information and only write the data once you've pressed **Ctrl+C**, which stops the process. Use this for around two minutes to get a record of what's going on.



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:55247        Windows:65001          ESTABLISHED
 [nvcontainer.exe]
  TCP    127.0.0.1:55366        Windows:55387          ESTABLISHED
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:55387        Windows:55366          ESTABLISHED
 [NVIDIA Share.exe]
  TCP    127.0.0.1:55407        Windows:55408          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55408        Windows:55407          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55414        Windows:55415          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55415        Windows:55414          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55416        Windows:55417          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55417        Windows:55416          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:65001        Windows:55247          ESTABLISHED
 [nvcontainer.exe]
  TCP    192.168.1.180:2869     bthub:35188            ESTABLISHED
 Can not obtain ownership information
  TCP    192.168.1.180:55255    db5sch101101426:https  ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    192.168.1.180:55406    8.36.113.113:https     ESTABLISHED
 [NVIDIA Share.exe]
  TCP    192.168.1.180:55409    imap:imap              ESTABLISHED
 [thunderbird.exe]
  TCP    192.168.1.180:55425    ec2-34-205-249-30:https  ESTABLISHED
 [firefox.exe]
  TCP    192.168.1.180:56449    imap:imap              ESTABLISHED
 [thunderbird.exe]
  TCP    192.168.1.180:56484    40.76.1.176:https      TIME_WAIT
  TCP    192.168.1.180:56485    40.76.1.176:https      TIME_WAIT
  TCP    192.168.1.180:56487    40.74.50.25:https      TIME_WAIT
  TCP    192.168.1.180:56488    65.55.44.109:https     ESTABLISHED
  DiagTrack
 [svchost.exe]
  TCP    [2a00:23c4:7588:5900:698e:541b:ccc7:d1e4]:55390  wo-in-x7d:5222         ESTABLISHED
 [googledrivesync.exe]
  TCP    [2a00:23c4:7588:5900:698e:541b:ccc7:d1e4]:55391  lhr25s12-in-x0a:https  CLOSE_WAIT
 [googledrivesync.exe]
  TCP    [2a00:23c4:7588:5900:698e:541b:ccc7:d1e4]:55395  lhr25s12-in-x0a:https  CLOSE_WAIT
 [googledrivesync.exe]
  TCP    [2a00:23c4:7588:5900:e8a1:c3d7:ba7b:bd17]:56359  wb-in-xbd:https        ESTABLISHED
```

```
C:\Windows\System32>cd\

C:\>md activity

C:\>cd activity

C:\activity>netstat -e -s -p tcp -b > activity1.txt

C:\activity>netstat -b 5 > activity2.txt
^C
C:\activity>
```

What is a Firewall?

The data packets that come and go between your PC and the outside world can be defined by a set of rules. These rules state whether a packet has access to the system in the first place, then whether or not it can gain access to its destination program. Collectively, these rules make up a Firewall.

Great Walls of Fire

The term firewall comes from fire prevention, where a physical wall is constructed in order to halt the spread of a fire. In digital terms, the physical wall stops malware and other threats from spreading into the system.

Some form of digital protection against unwanted entry into a system has existed for many years but the more recent software side of a firewall, one that we're reasonably familiar with, has only been around since the '80s.

Prior to the modern firewall, system administrators blocked unwanted access through various stages of hardware layers. Long lists of allowed computer addresses were painstakingly entered into mainframes and routers, where programmable chips filtered the white list and simply stopped all access to addresses that weren't on the list; think of a nightclub bouncer, if your name's not on the list you're not getting in.

In its simplest guise, a firewall will look to a defined set of rules then apply those rules to any data packets that pass through it. For example, if you've created a rule whereby all Telnet traffic is blocked, any packet that's trying to reach port 23, the port that Telnet applications listen on for data, will be blocked. While suitably effective this low-level packet filtering does have its Achilles heel, in that it treats each packet as an independent piece of data: not knowing whether it's a part of an already established stream of data. This can be targeted by hackers who want access to a system with a firewall in place. The clever hacker is able to spoof a packet and thus tricking the firewall into letting it pass. It takes some time, and it's a bit hit and miss, but most hackers have plenty of patience when it comes to getting into a network. Therefore a much needed higher degree of firewall monitoring is called for.

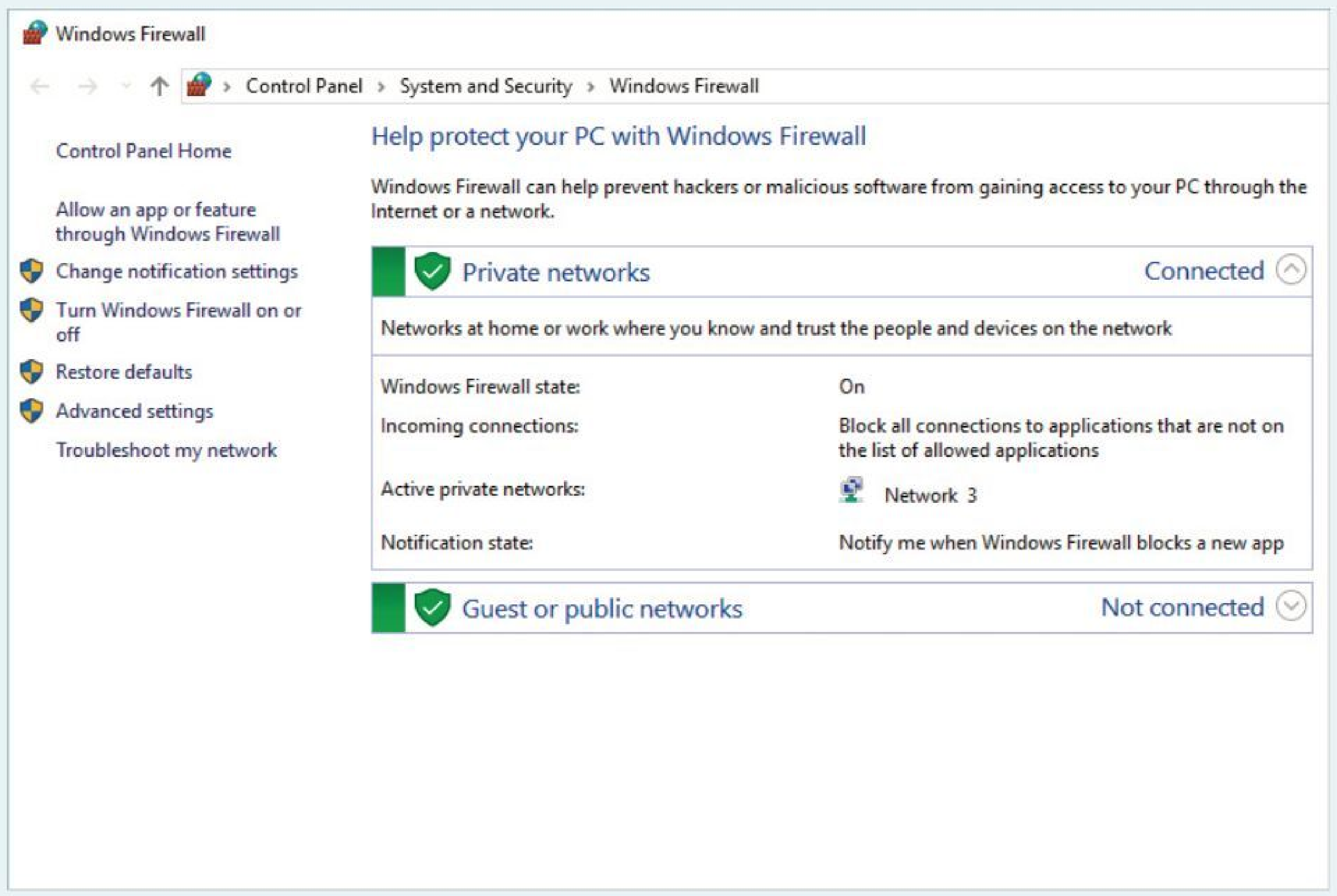
Stateful Inspection firewalls were introduced in the mid '90s and enabled a firewall to log all the connection that passed through it determining what was the start of a new packet stream, part of an existing packet stream or something random. This allows a firewall to allow or drop any access based on a data packet's history. In terms of effectiveness, this makes the firewall more efficient and faster at dealing with connection requests as it doesn't need to continually analyse each packet as an individual but rather as a whole stream. For added layers of protection, if a packet doesn't match any of the connection histories, then it can be evaluated and filtered through the various rules to determine its legitimacy.

A further layer of protection was included into the basic firewall early in the 2000s. Application-layer analysis enabled firewalls to inspect packets that were targeting individual applications within the operating system. Each program or application installed in the system will use a set of protocols to communicate with the outside world. When an application is installed, on a Windows 10 system for example, the installation mechanism will automatically add an instance of it to the Windows 10 firewall. This means that it is able to send and receive information successfully through the Windows firewall without any of it being blocked. By blocking an application's access to the outside world, the user could miss out on regular updates, fixes, patches and so on. One of the key benefits to an application-layer firewall is that it's excellent at blocking specific content, such as known malware and viruses or dangerous websites. It's also capable of determining when a particular protocol is being misused by a rogue application.

Where the firewall proceeds from this point is unclear. However many experts agree that although we'll always need a firewall, the modern systems, networks and devices have so many potential access points that it's fast becoming less efficient to run the standard firewall model. In effect, the modern firewall, regardless of how complex and efficient it has become over the years, is quick becoming a bottle-neck for the operating system. What some experts are theorising is that at some point in the future, the need for a single, overall firewall will be outdated and that the next-generation operating systems will require each program and application that can be installed to act as its own firewall. Whether this will come about is pure fantasy at the moment but at the speed digital technologies grow and evolve there's a good chance of finding out soon enough.

> *Hardware firewalls are an early example of network security*

LAN
WAN
USB
CONSOLE
POWER
RESET



Windows Firewall

Control Panel › System and Security › Windows Firewall

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

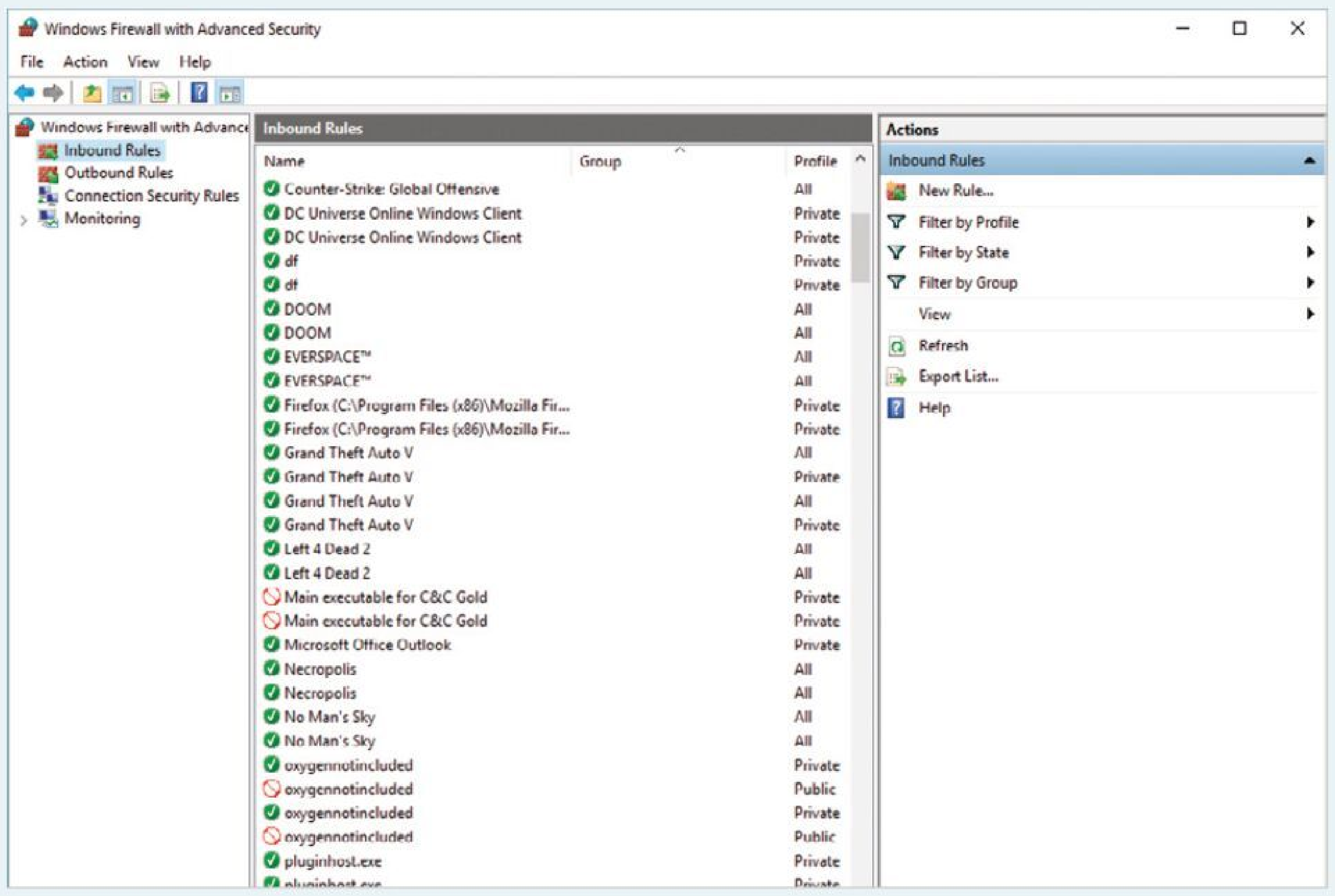
Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to applications that are not on the list of allowed applications
Active private networks:	Network 3
Notification state:	Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

"The built-in Windows 10 firewall is certainly good enough for most users' needs. It's fast, effective and can be easily configured."



Windows Firewall with Advanced Security

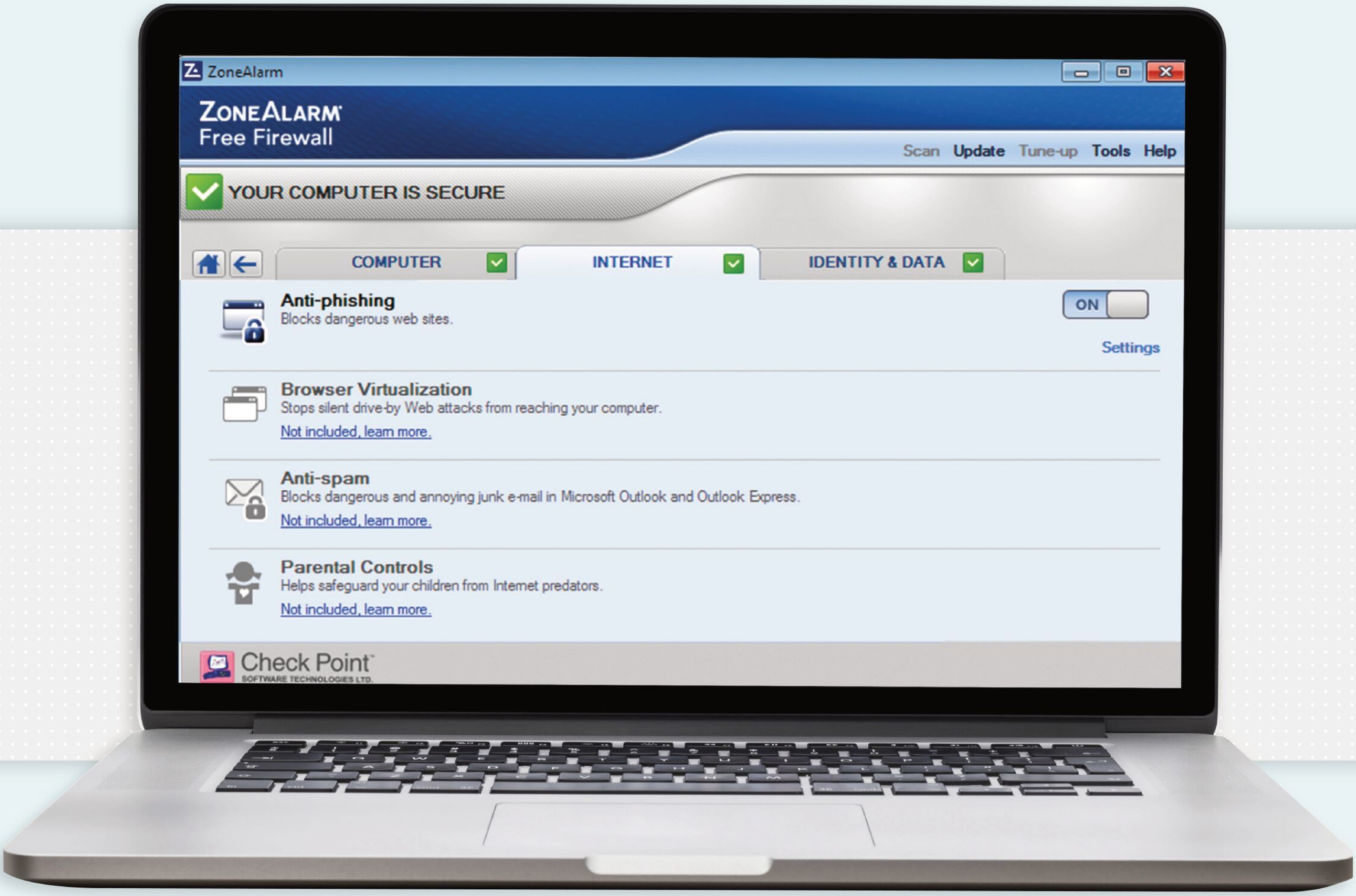
Inbound Rules

Name	Group	Profile
Counter-Strike: Global Offensive		All
DC Universe Online Windows Client		Private
DC Universe Online Windows Client		Private
df		Private
df		Private
DOOM		All
DOOM		All
EVERSPACE™		All
EVERSPACE™		All
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private
Grand Theft Auto V		All
Grand Theft Auto V		Private
Grand Theft Auto V		All
Grand Theft Auto V		Private
Left 4 Dead 2		All
Left 4 Dead 2		All
Main executable for C&C Gold		Private
Main executable for C&C Gold		Private
Microsoft Office Outlook		Private
Necropolis		All
Necropolis		All
No Man's Sky		All
No Man's Sky		All
oxygennotincluded		Private
oxygennotincluded		Public
oxygennotincluded		Private
oxygennotincluded		Public
pluginhost.exe		Private

File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refrech
Export List...
Help

"When each program, application, game and so on is installed, it is entered into the Windows 10 firewall so it can communicate with the outside world."

"There are countless freely available third-party firewalls clients. Some are very good, others not so much."



ZoneAlarm

YOUR COMPUTER IS SECURE

Anti-phishing
Blocks dangerous web sites.

Browser Virtualization
Stops silent drive-by Web attacks from reaching your computer.
Not included, learn more.

Anti-spam
Blocks dangerous and annoying junk e-mail in Microsoft Outlook and Outlook Express.
Not included, learn more.

Parental Controls
Helps safeguard your children from Internet predators.
Not included, learn more.

ZoneAlarm Free Firewall
Scan
Update
Tune-up
Tools
Help
COMPUTER
INTERNET
IDENTITY & DATA
ON
Settings
Check Point SOFTWARE TECHNOLOGIES LTD.

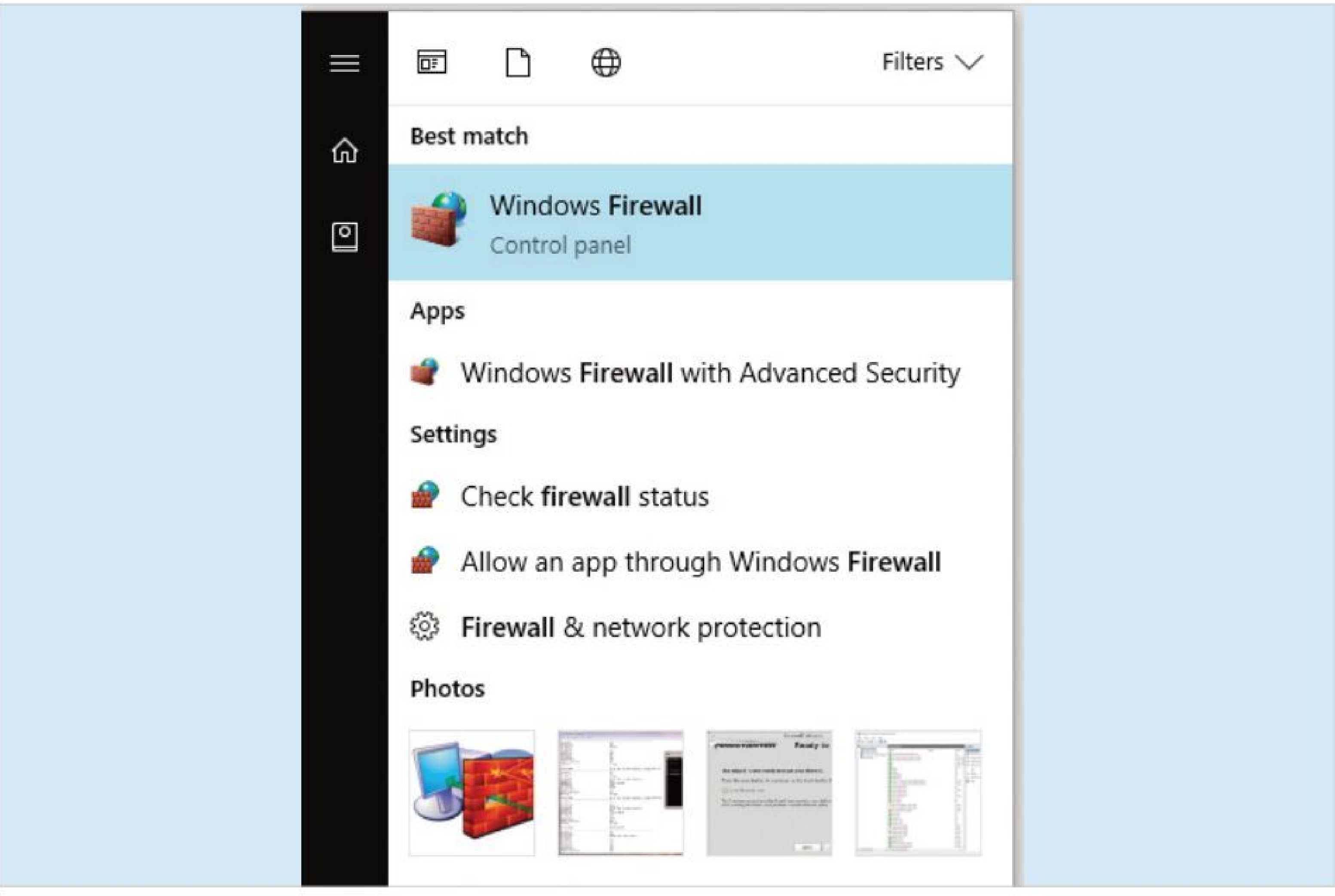
Improving the Windows 10 Firewall

The built-in Windows 10 firewall is a surprisingly good security application. Whilst it may not be as efficient as something offered by one of the third-party security suites, it's certainly more than adequate for the average user.

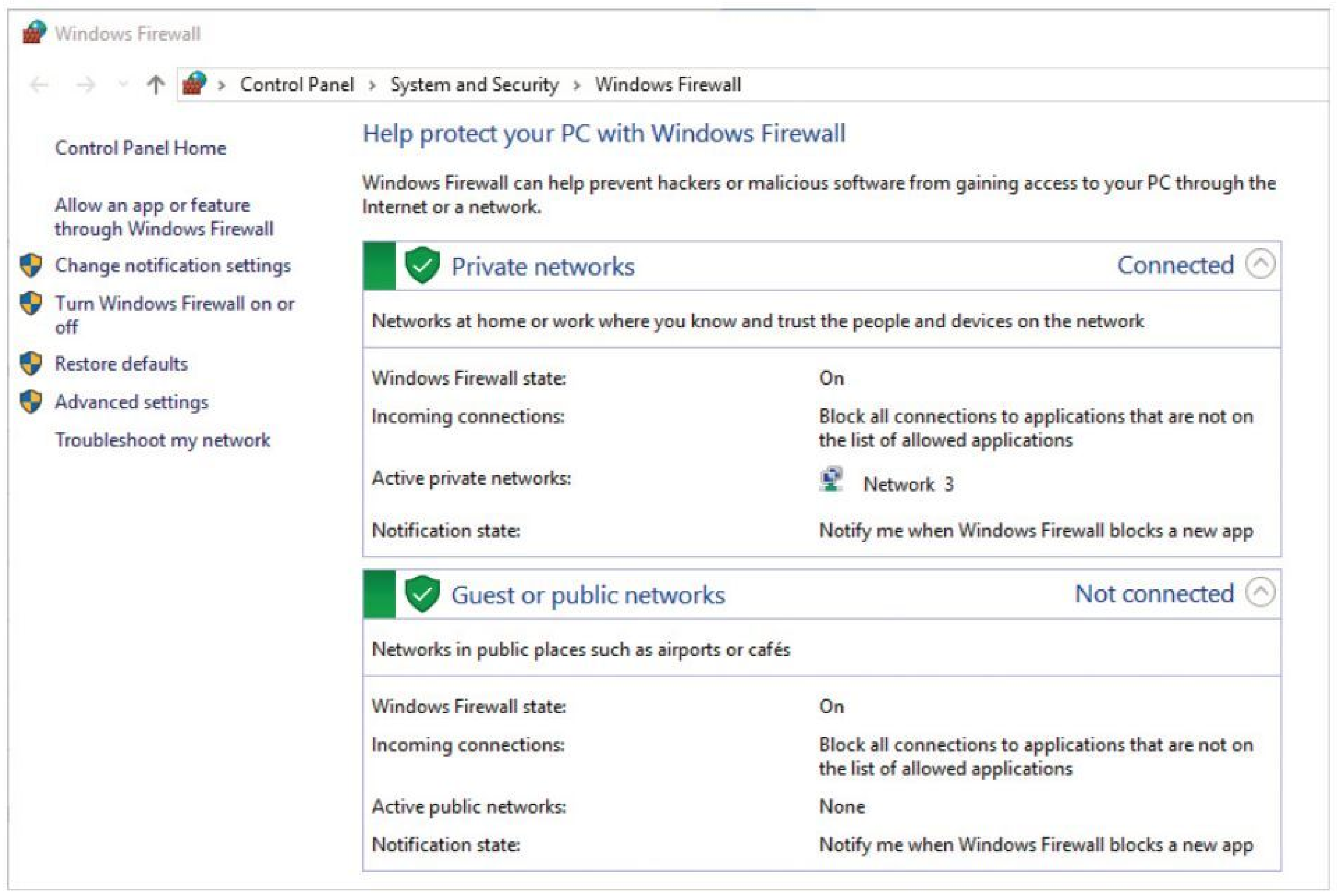
Getting to Know Your Firewall

Generally, there's little need to ever configure the Windows 10 firewall. However, getting to know how it works and improving it is part of being more security-conscious. Here's some tips on how to manage it better.

STEP 1 You can open the main Windows 10 firewall console window by clicking on the Windows Start button and entering firewall into the search box. Click the returned link, Windows Firewall Control Panel, to launch it.


Filters
Best match
Windows Firewall
Control panel
Apps
Windows Firewall with Advanced Security
Settings
Check firewall status
Allow an app through Windows Firewall
Firewall & network protection
Photos

STEP 2 The Windows 10 firewall console window starts by detailing the basic status of the firewall. It should be On by default, unless you've installed a third-party security suite which contains its own firewall. There are two kinds of network listed, Private and Public. Private is for home or work, whereas Public is for cafés and the like.


Windows Firewall
Control Panel › System and Security › Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

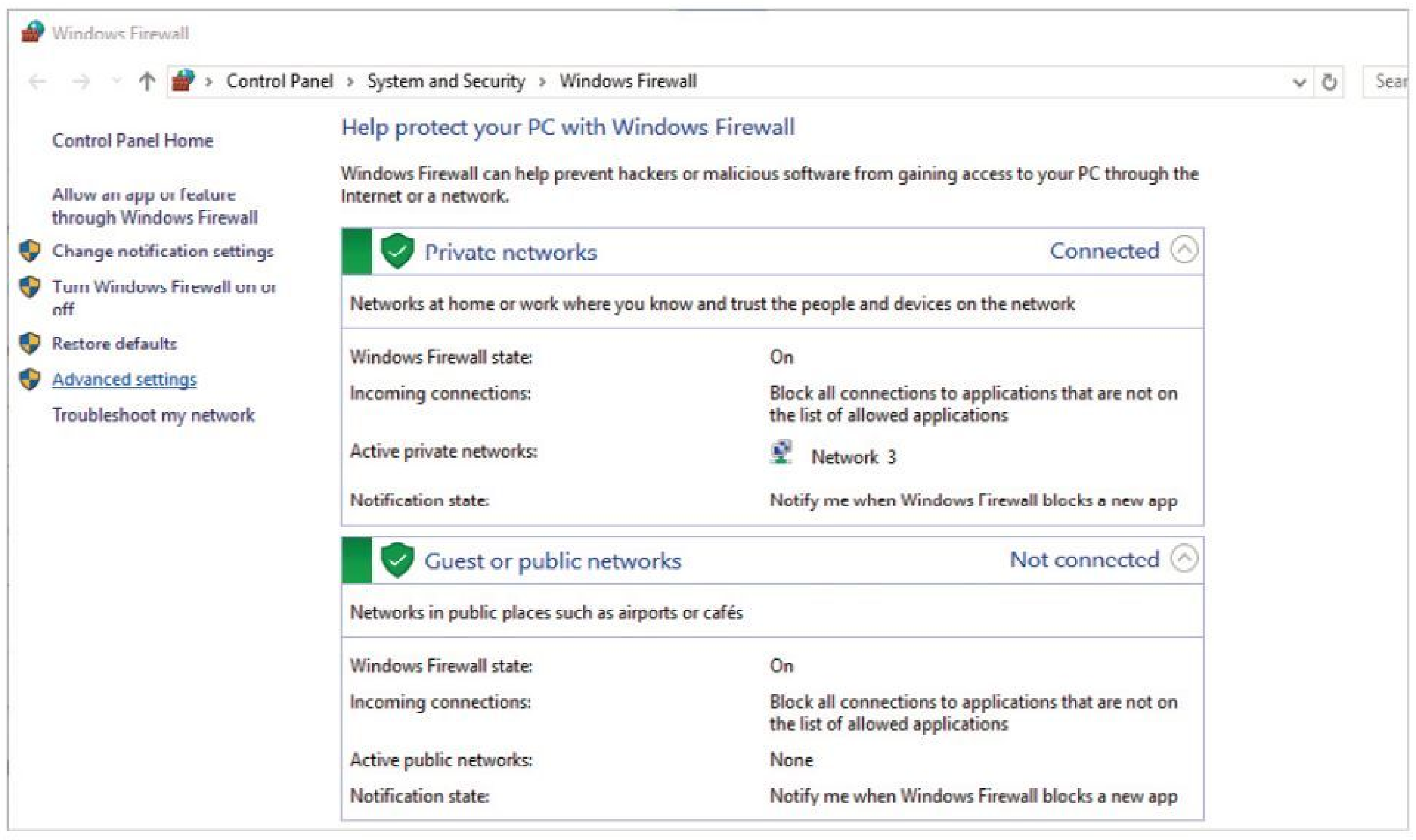
Windows Firewall state: On
Incoming connections: Block all connections to applications that are not on the list of allowed applications
Active private networks: Network 3
Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

Networks in public places such as airports or cafés

Windows Firewall state: On
Incoming connections: Block all connections to applications that are not on the list of allowed applications
Active public networks: None
Notification state: Notify me when Windows Firewall blocks a new app

STEP 3 Down the left-hand side are some links that will help you configure and improve the firewall, as well as turning it on or off (which isn't recommended under any circumstance other than the installation of an improved third-party firewall). To begin with, start by clicking on the Advanced Settings link.


Windows Firewall
Control Panel › System and Security › Windows Firewall
Sear
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

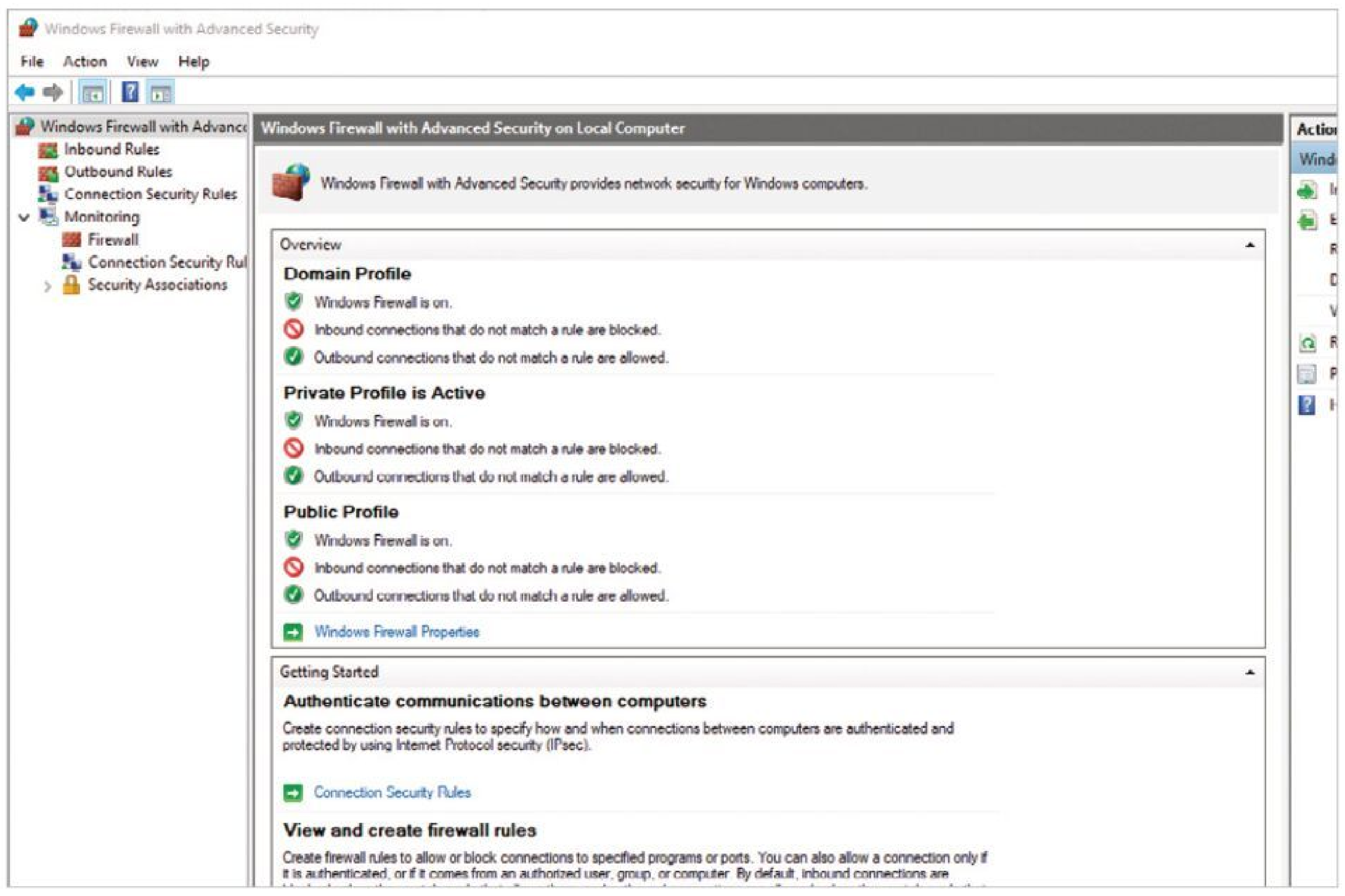
Windows Firewall state: On
Incoming connections: Block all connections to applications that are not on the list of allowed applications
Active private networks: Network 3
Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

Networks in public places such as airports or cafés

Windows Firewall state: On
Incoming connections: Block all connections to applications that are not on the list of allowed applications
Active public networks: None
Notification state: Notify me when Windows Firewall blocks a new app

STEP 4 The Advanced Settings link launches a new console window. This new console defines the inbound and outbound rules for the entire system and its installed programs and applications. You can set authentication rules between computers, view and create new firewall rules, view the current firewall policies and even monitor what's being blocked in realtime.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rul
Security Associations
Actio
Wind
Windows Firewall with Advanced Security on Local Computer
Overview
Getting Started

Windows Firewall with Advanced Security provides network security for Windows computers.

Domain Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Private Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Public Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Authenticate communications between computers

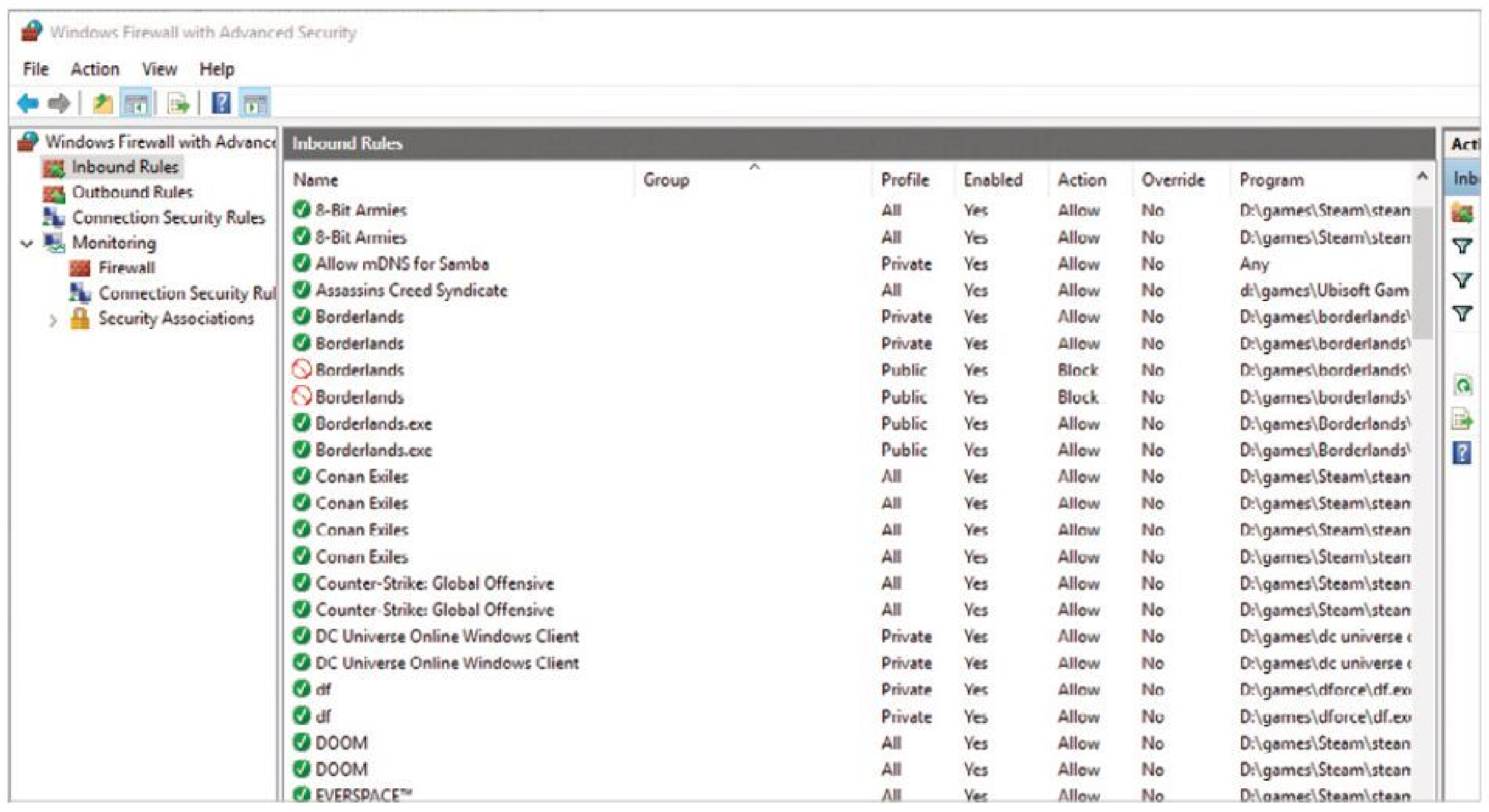
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

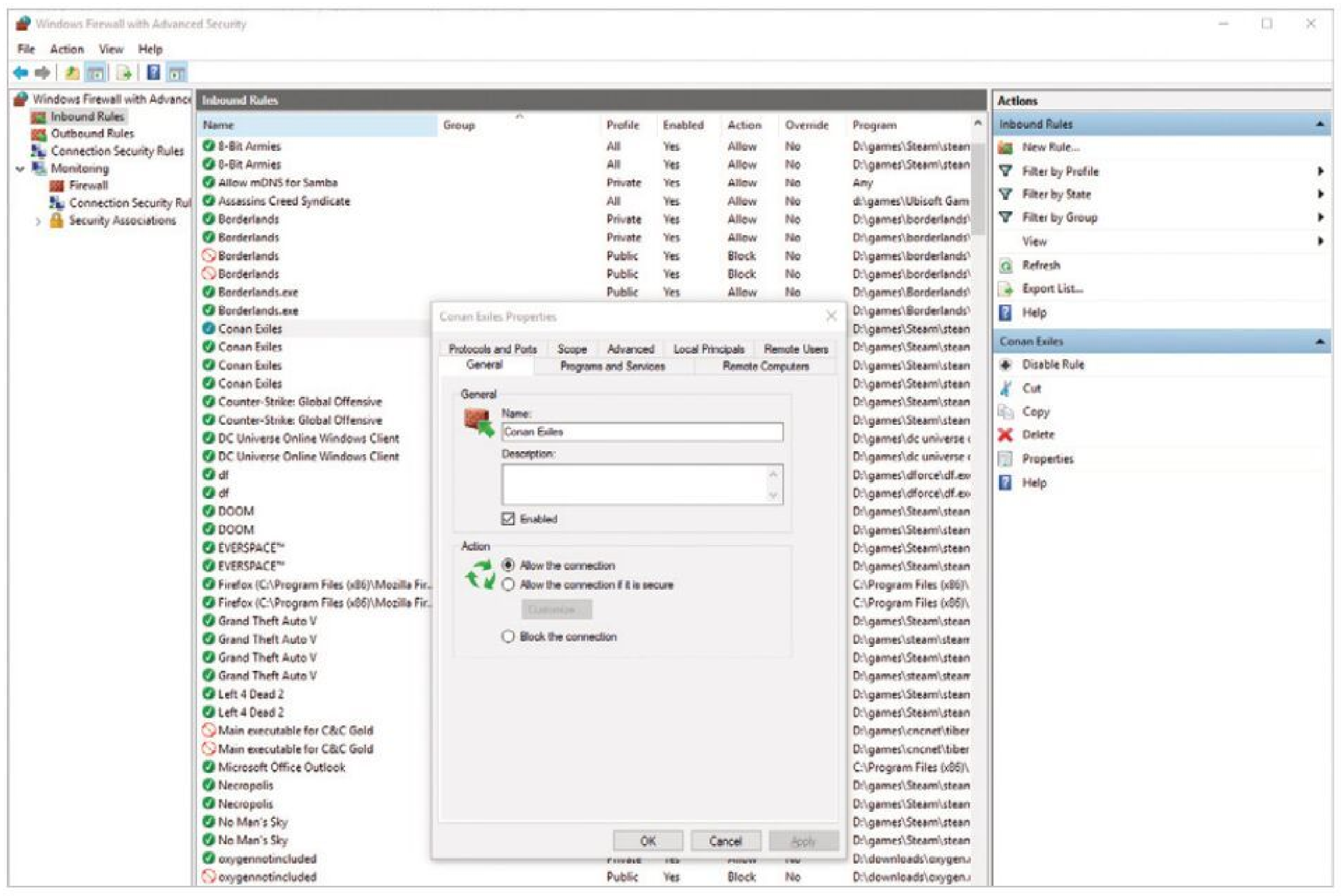
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are

STEP 5 Click on Inbound Rules to the right-hand side of the main console window. This will list the current rules that allow traffic into your computer and to the applications that require it. For example, in this screenshot there are rules for various games that allow multiplayer interaction and the ability to 'talk' to the game server as well as install updates.

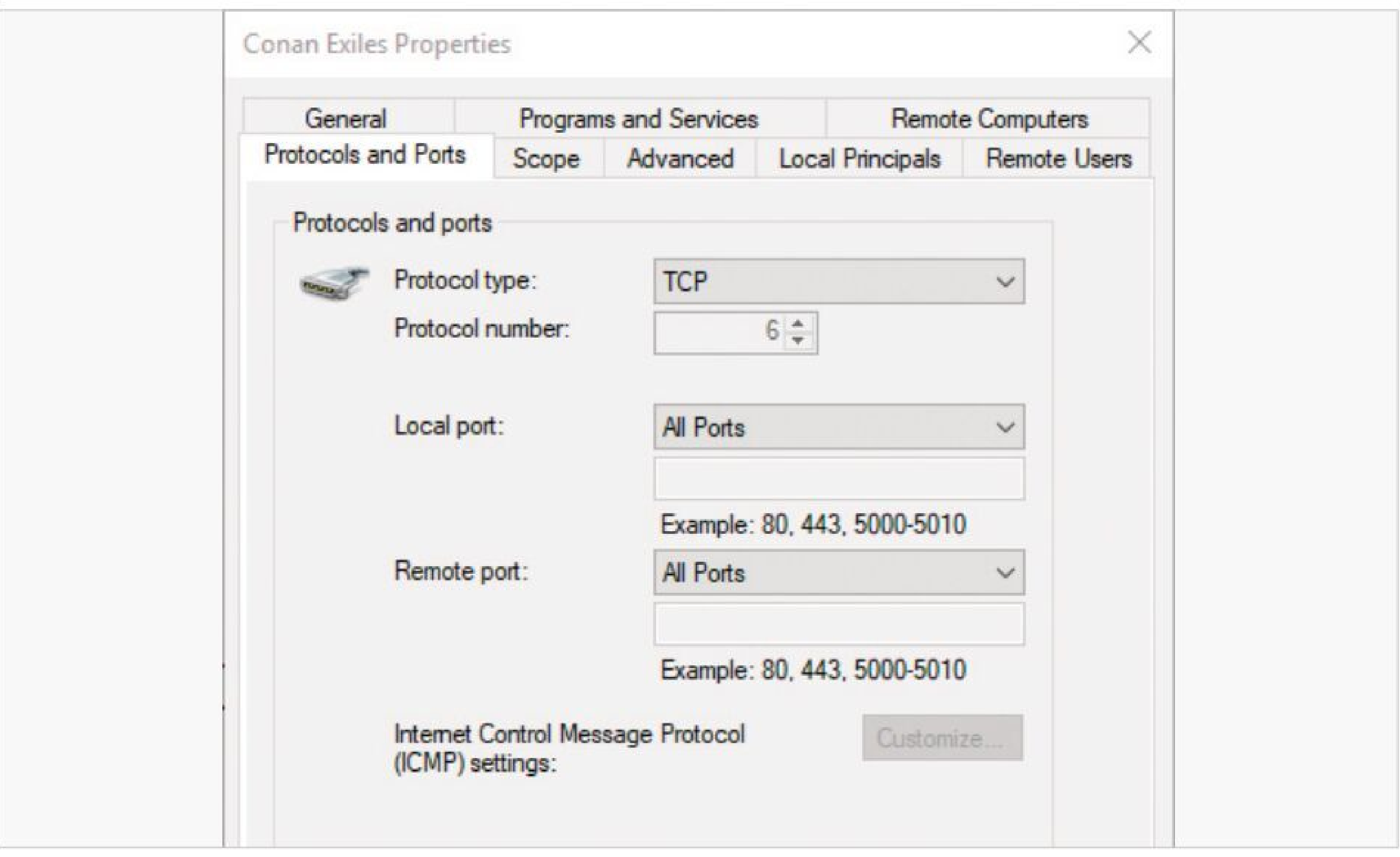

Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rul
Security Associations
Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program
8-Bit Armies		All	Yes	Allow	No	D:\games\Steam\stean
8-Bit Armies		All	Yes	Allow	No	D:\games\Steam\stean
Allow mDNS for Samba		Private	Yes	Allow	No	Any
Assassins Creed Syndicate		All	Yes	Allow	No	d:\games\Ubisoft Gam
Borderlands		Private	Yes	Allow	No	D:\games\borderlands\
Borderlands		Private	Yes	Allow	No	D:\games\borderlands\
Borderlands		Public	Yes	Block	No	D:\games\borderlands\
Borderlands		Public	Yes	Block	No	D:\games\borderlands\
Borderlands.exe		Public	Yes	Allow	No	D:\games\Borderlands\
Borderlands.exe		Public	Yes	Allow	No	D:\games\Borderlands\
Conan Exiles		All	Yes	Allow	No	D:\games\Steam\stean
Conan Exiles		All	Yes	Allow	No	D:\games\Steam\stean
Conan Exiles		All	Yes	Allow	No	D:\games\Steam\stean
Conan Exiles		All	Yes	Allow	No	D:\games\Steam\stean
Counter-Strike: Global Offensive		All	Yes	Allow	No	D:\games\Steam\stean
Counter-Strike: Global Offensive		All	Yes	Allow	No	D:\games\Steam\stean
DC Universe Online Windows Client		Private	Yes	Allow	No	D:\games\dc universe (
DC Universe Online Windows Client		Private	Yes	Allow	No	D:\games\dc universe (
df		Private	Yes	Allow	No	D:\games\dforce\df.ex
df		Private	Yes	Allow	No	D:\games\dforce\df.ex
DOOM		All	Yes	Allow	No	D:\games\Steam\stean
DOOM		All	Yes	Allow	No	D:\games\Steam\stean
EVERSPACE™		All	Yes	Allow	No	D:\games\Steam\stean

STEP 6 These rules are automatically entered into the firewall when you install the program, game or app. When you install a program you're required to accept and authenticate the process, clicking on Yes to start the installation. This level of administrative access also allows entry of the program into the firewall. Pick one of the entries and double-click it.

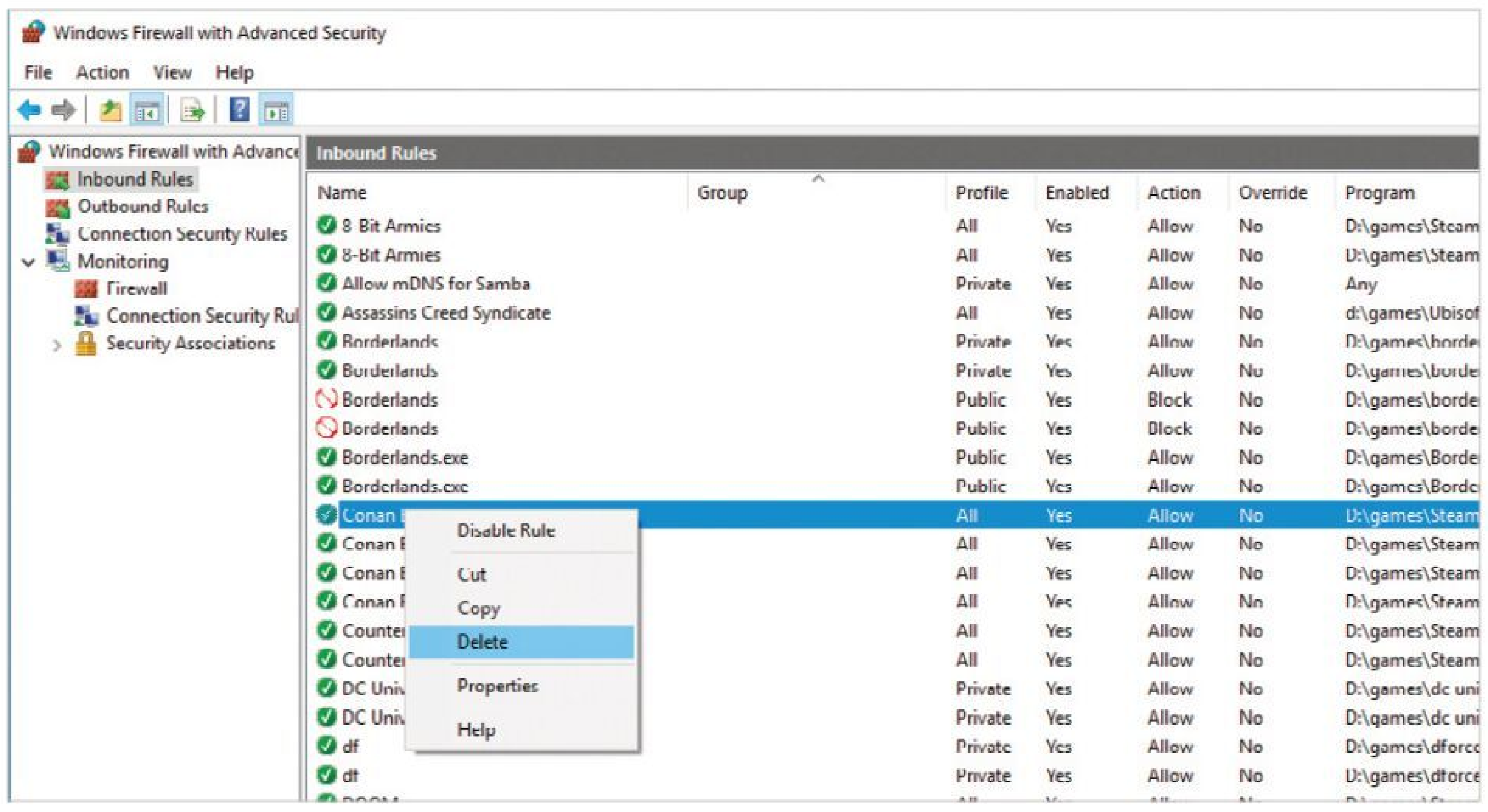


STEP 7 The properties of each firewall entry allow a greater degree of control for that particular program. You can change the name of the entry, allow or block the connection, define the physical location of the program on your computer, allow access to the program from remote computers, set the protocol and port number it uses and even which network controller to use.


Conan Exiles Properties
General
Programs and Services
Remote Computers
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
Protocols and ports
Internet Control Message Protocol (ICMP) settings:
Customize...

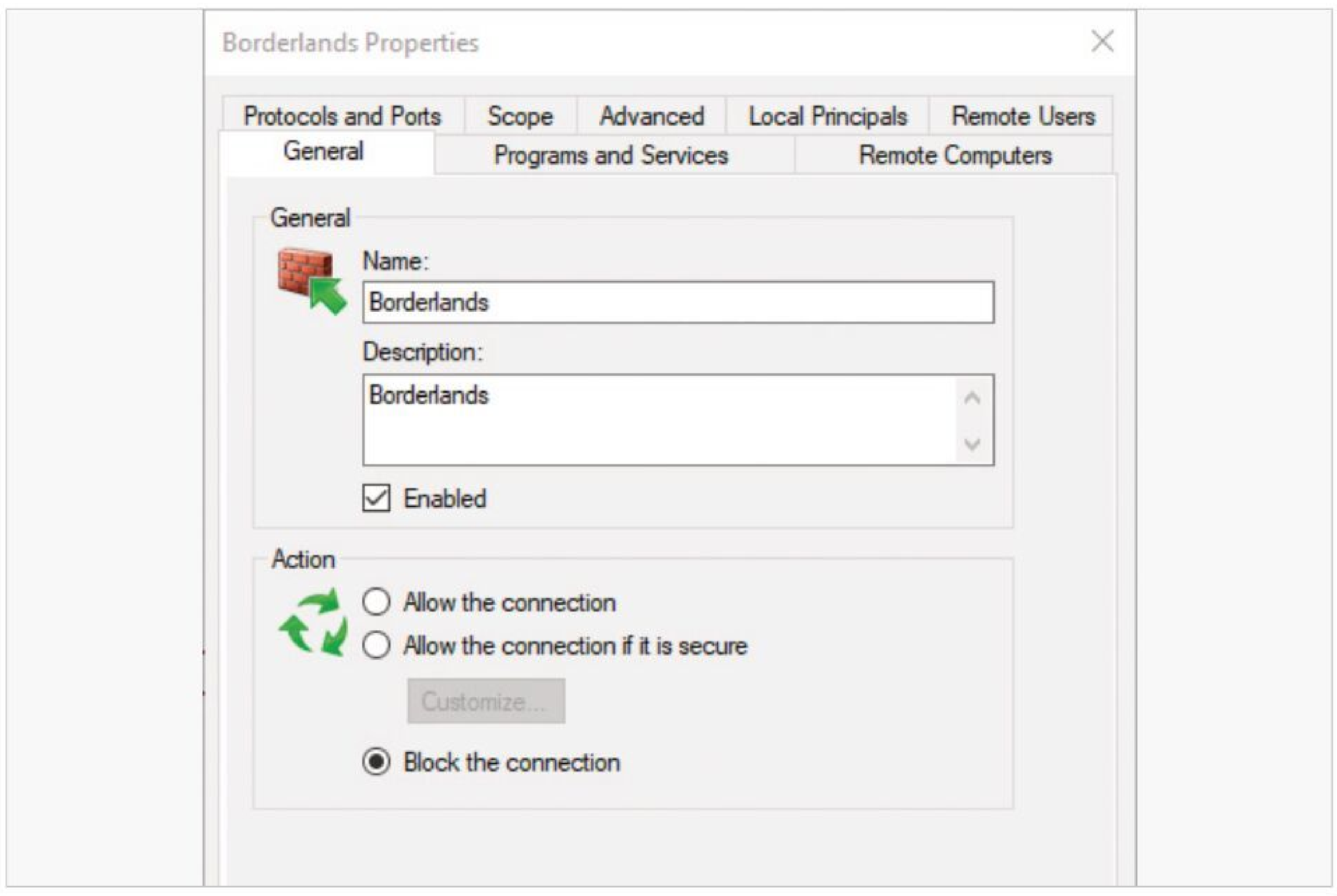
Protocol type: TCP
Protocol number: 6
Local port: All Ports
Example: 80, 443, 5000-5010
Remote port: All Ports
Example: 80, 443, 5000-5010

STEP 8 Sometimes, uninstalling a program doesn't automatically remove it from the Windows firewall. The exact reasons why are varied but to help improve the efficiency of the Windows firewall, whenever you remove a program from your system, it's worth checking the firewall to see if its entry has been deleted. To delete an entry, right-click then select Delete from the menu.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rul
Security Associations
Inbound Rules
Disable Rule
Cut
Copy
Delete
Properties
Help

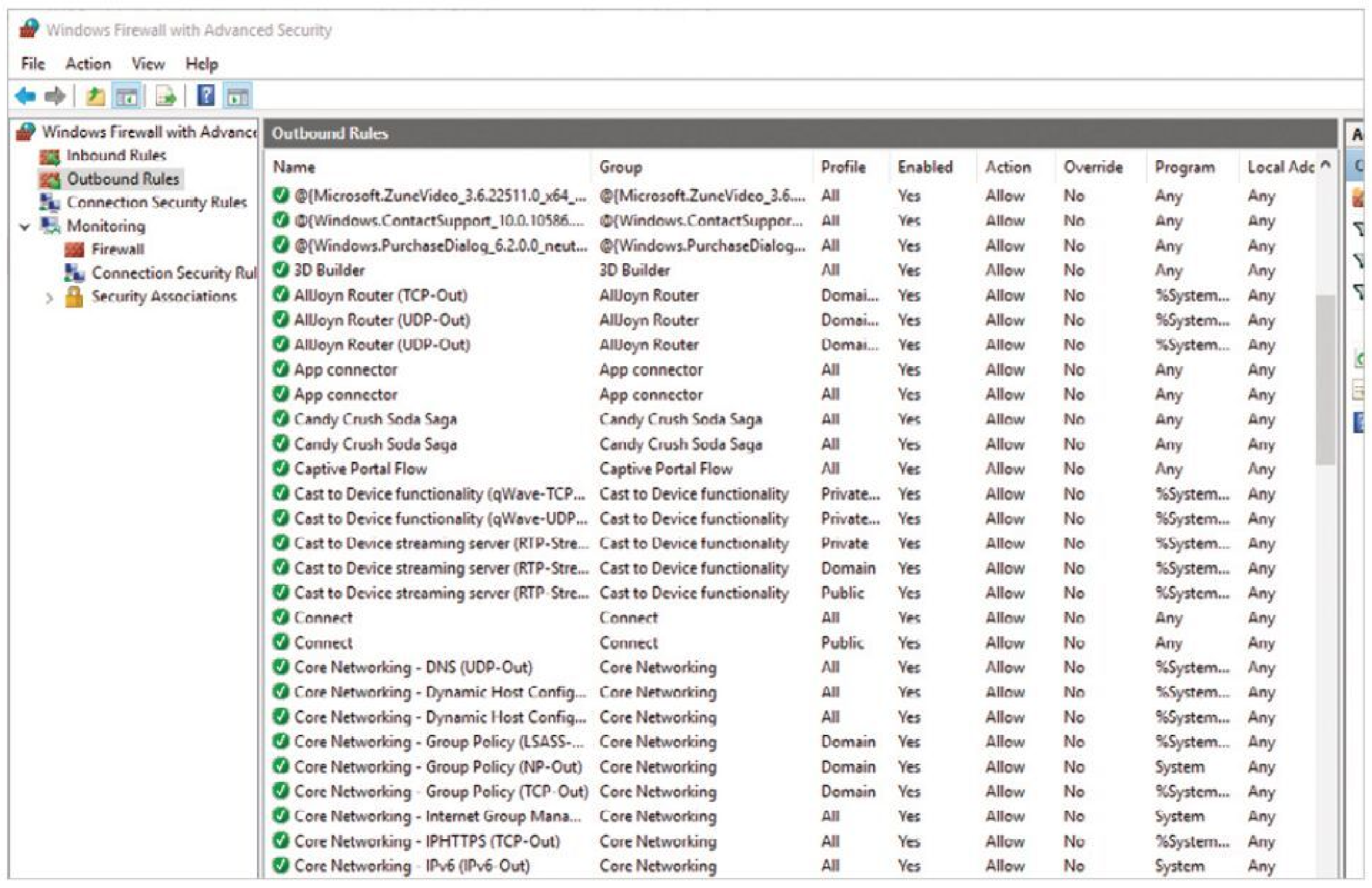
Name	Group	Profile	Enabled	Action	Override	Program
8 Bit Armies		All	Yes	Allow	No	D:\games\Steam
8-Bit Armies		All	Yes	Allow	No	D:\games\Steam
Allow mDNS for Samba		Private	Yes	Allow	No	Any
Assassins Creed Syndicate		All	Yes	Allow	No	d:\games\Ubisof
Borderlands		Private	Yes	Allow	No	D:\games\borde
Borderlands		Private	Yes	Allow	No	D:\games\borde
Borderlands		Public	Yes	Block	No	D:\games\borde
Borderlands		Public	Yes	Block	No	D:\games\borde
Borderlands.exe		Public	Yes	Allow	No	D:\games\Borde
Borderlands.exe		Public	Yes	Allow	No	D:\games\Borde
Conan E		All	Yes	Allow	No	D:\games\Steam
Conan E		All	Yes	Allow	No	D:\games\Steam
Conan E		All	Yes	Allow	No	D:\games\Steam
Conan E		All	Yes	Allow	No	D:\games\Steam
Counter		All	Yes	Allow	No	D:\games\Steam
Counter		All	Yes	Allow	No	D:\games\Steam
DC Univ		Private	Yes	Allow	No	D:\games\dc uni
DC Univ		Private	Yes	Allow	No	D:\games\dc uni
df		Private	Yes	Allow	No	D:\games\dforce
df		Private	Yes	Allow	No	D:\games\dforce

STEP 9 You may not want to delete a rule as it could be used later or if you reinstall the program and it fails to recreate the firewall entry. The recommended process then is to block the rule from communicating with the outside world. To do this, double-click the rule and from the General tab click the Block the connection button.


Borderlands Properties
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
General
Programs and Services
Remote Computers
General
Action
Customize...

Name: Borderlands
Description: Borderlands
☑ Enabled
○ Allow the connection
○ Allow the connection if it is secure
● Block the connection

STEP 10 Similarly, the Outbound Rules link will detail the various programs that are allowed to communicate from your computer to an external destination. It's good practise to familiarise yourself with the rules of the firewall, as a rogue program will need to set a rule to communicate. You can then block that rule and stop the threat from reporting back.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rul
Security Associations
Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Adc
@{Microsoft.ZuneVideo_3.6.22511.0_x64_...	@{Microsoft.ZuneVideo_3.6....	All	Yes	Allow	No	Any	Any
@{Windows.ContactSupport_10.0.10586....	@{Windows.ContactSuppor...	All	Yes	Allow	No	Any	Any
@{Windows.PurchaseDialog_6.2.0.0_neut...	@{Windows.PurchaseDialog...	All	Yes	Allow	No	Any	Any
3D Builder	3D Builder	All	Yes	Allow	No	Any	Any
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
App connector	App connector	All	Yes	Allow	No	Any	Any
App connector	App connector	All	Yes	Allow	No	Any	Any
Candy Crush Soda Saga	Candy Crush Soda Saga	All	Yes	Allow	No	Any	Any
Candy Crush Soda Saga	Candy Crush Soda Saga	All	Yes	Allow	No	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any
Connect	Connect	All	Yes	Allow	No	Any	Any
Connect	Connect	Public	Yes	Allow	No	Any	Any
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Group Policy (LSASS-...	Core Networking	Domain	Yes	Allow	No	%System...	Any
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System	Any
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	System	Any

Creating a Security Plan

A security plan will help you form a better strategy when it comes to tackling your Windows and home network security. A good plan will help keep on top of backups, updates and possible areas of weakness that malware or hackers can exploit.

Plan for the Worst, Hope for the Best

There's a lot to consider when coming up with a good security plan. It's not just a case of occasionally checking for an OS update on your own computer, you have to take into account other computers and the entire network.

An effective security plan should encompass the whole of your network, which includes Windows computers, Android and iOS devices, your router, any powerline adapters, Wi-Fi coverage, access passwords and even where the Ethernet cable runs through.

It may sound a little extreme but like most checklist-type scenarios it can be as in-depth as you like. However, it's worth at least considering some aspects of the home network and overall security before starting a plan.

"Users form the most vulnerable point of access for security on any system. Educate and make sure they're safe."

Users

More than likely the 'user' is the most vulnerable point of access and the biggest security threat to any system or network. Whilst you can have the greatest AV suite and water-tight security system in the world, the user who carelessly visits unbeliveableandobviouslyfakedeals.com is the one that's going to cause you the most headaches. In a home network that's often youngsters, those who don't quite understand the whole Internet security element.

Whilst most youngsters are more tech-savvy than us adults, there's an age range where they'll happily click a link from a friend or something they've seen that looks cool. Therefore take the time to educate and frequently check their accounts or computers for anything suspicious. If possible enforce limits to their browsing and regularly update the browsing rules to make sure they're not going where they shouldn't. Remember, it's not just viruses that a child can download, they could potentially see something that would affect them emotionally.

Updates

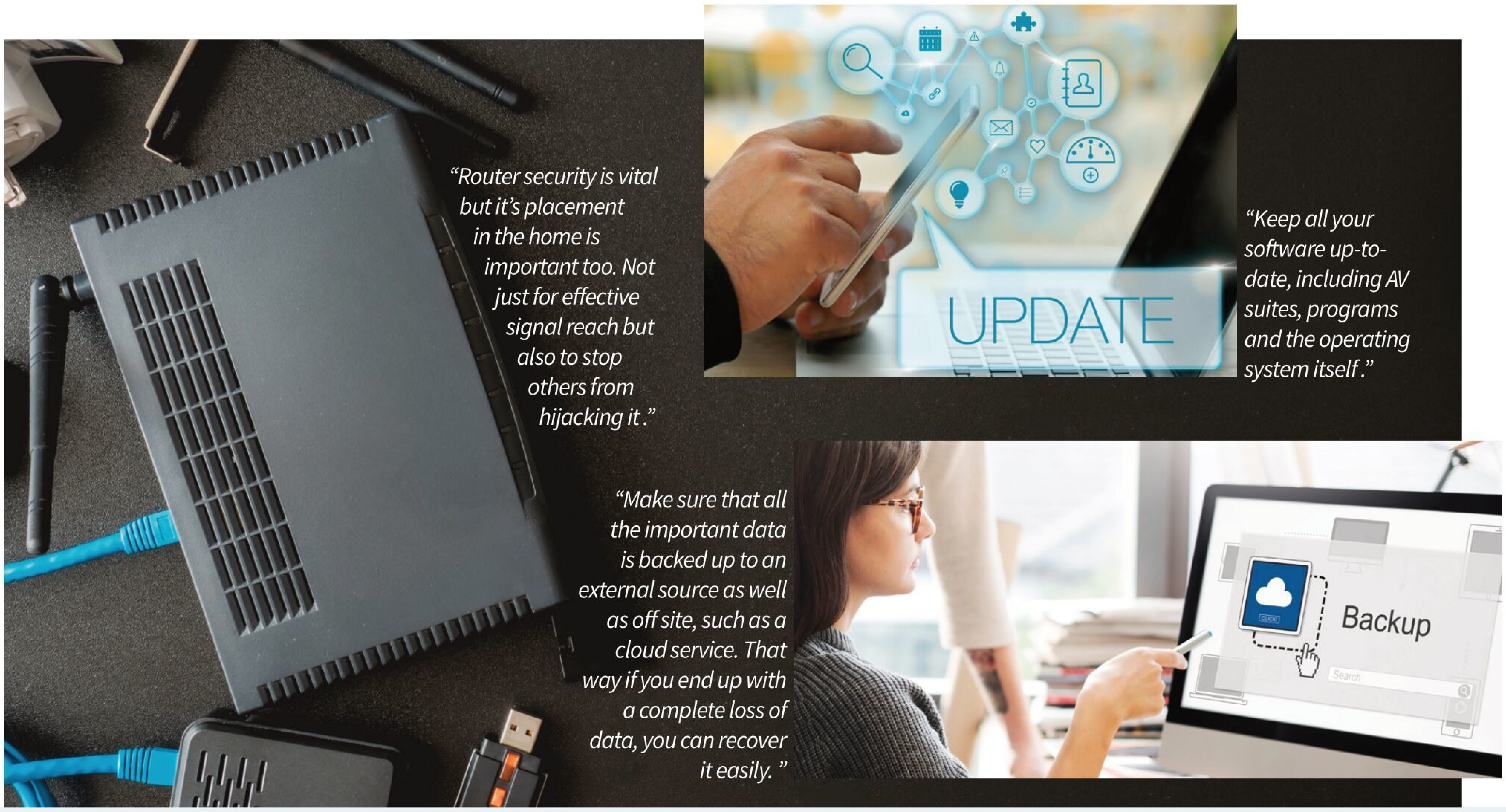
Obviously a must-have section of a good security plan is to regularly check for system and program updates. Thankfully, Windows 10 and most security suites will run an automatic check whenever the system is powered up and connected to the Internet. However, there's always some point where an update failed to initialise for some reason or another. Therefore, it's often best to manually check.

Consider too checking for updates for the most frequently used programs. Microsoft Office, GIMP, your browser and even games will inevitably have an update available which can enhance, protect and improve the security of the program. After that, make sure that the other installed programs on the system are up-to-date too, as it's best to make sure there's few weaknesses as possible.

Programs

It can be difficult to keep track of what programs are installed on a system but it's not impossible. If you're serious about the security of your home network and its systems, then taking stock of what programs are installed on each system is worth doing.

Running through a checklist of installed programs you may notice one that shouldn't be there. A quick lookup of the program may reveal that it's a popular backdoor for hackers to get into a system and the attached network. That being the case, it needs to be removed and any firewall entries checked and disabled.



"Router security is vital but it's placement in the home is important too. Not just for effective signal reach but also to stop others from hijacking it."

"Keep all your software up-to-date, including AV suites, programs and the operating system itself."

"Make sure that all the important data is backed up to an external source as well as off site, such as a cloud service. That way if you end up with a complete loss of data, you can recover it easily."

Routers

The family router is the first point of access for anything malicious on the network, since it's the gateway to the outside world. Make sure that the router software is up-to-date and that it's using the best possible wireless security standards and encryption.

It's also beneficial to make sure that the router's admin password and access passwords are hidden from sight. It doesn't take much for someone to look through the front window and make a note of a router password that's carelessly on show for all to see. Consider too, that not all visitors to your home are going to be chivalrous towards viewing your network password.

It's also worth tracking the range of the wireless signal from the router. By installing and using a good Wi-Fi scanner on a mobile device you can tell where the Wi-Fi signal from your router lies beyond your home. Whilst it's good to have a powerful signal, it won't take much for someone to sit nearby with a laptop (or a neighbour) and hack into your network. A Wi-Fi analyser will help you determine the best placement for security and more efficient use of the signal.

Passwords

It's not common for a home user to frequently change their password to the same degree as would an office worker but it's certainly something worth implementing. Using a combination of a good password manager and generator, you can set a 30-day password limit for all users and their access to the sites they visit.

It might sound like an awful lot of hard work on the part of everyone involved but weak passwords and the same password being used across Facebook, banking and gaming is a huge security vulnerability.

Backups

We'll cover backups in a few pages time but for the meantime though making sure that each account and computer is regularly backed up can take much stress out of a security situation. If you're unlucky enough to catch a virus or other malware, or are unfortunate enough to be hacked, you'll need to act quickly to prevent any loss of personal information. This usually means wiping your computer completely.

Having a good and reliable backup solution will help you recover your valuable data in no time, should you ever need to wipe everything or all your data is compromised through malware. It's also worth thinking of investing in a fireproof safe to store your backups along with cloud options for off-site backup security.

Cabling

It's not always something you need to check but ensuring that the home's Ethernet cabling is secure is an essential element to network security. For example, if you live in shared accommodation, it's possible for a neighbour to be able to be able to connect to your Ethernet cable and steal your bandwidth or gain access to your network resources.

If you can implement all or just some of these elements into your plan, you will be well on the way to making sure that your home network is as secure as possible, without becoming too paranoid over potential threats from outside sources. After all, you lock your doors when you're not at home so why shouldn't you lock your network too.

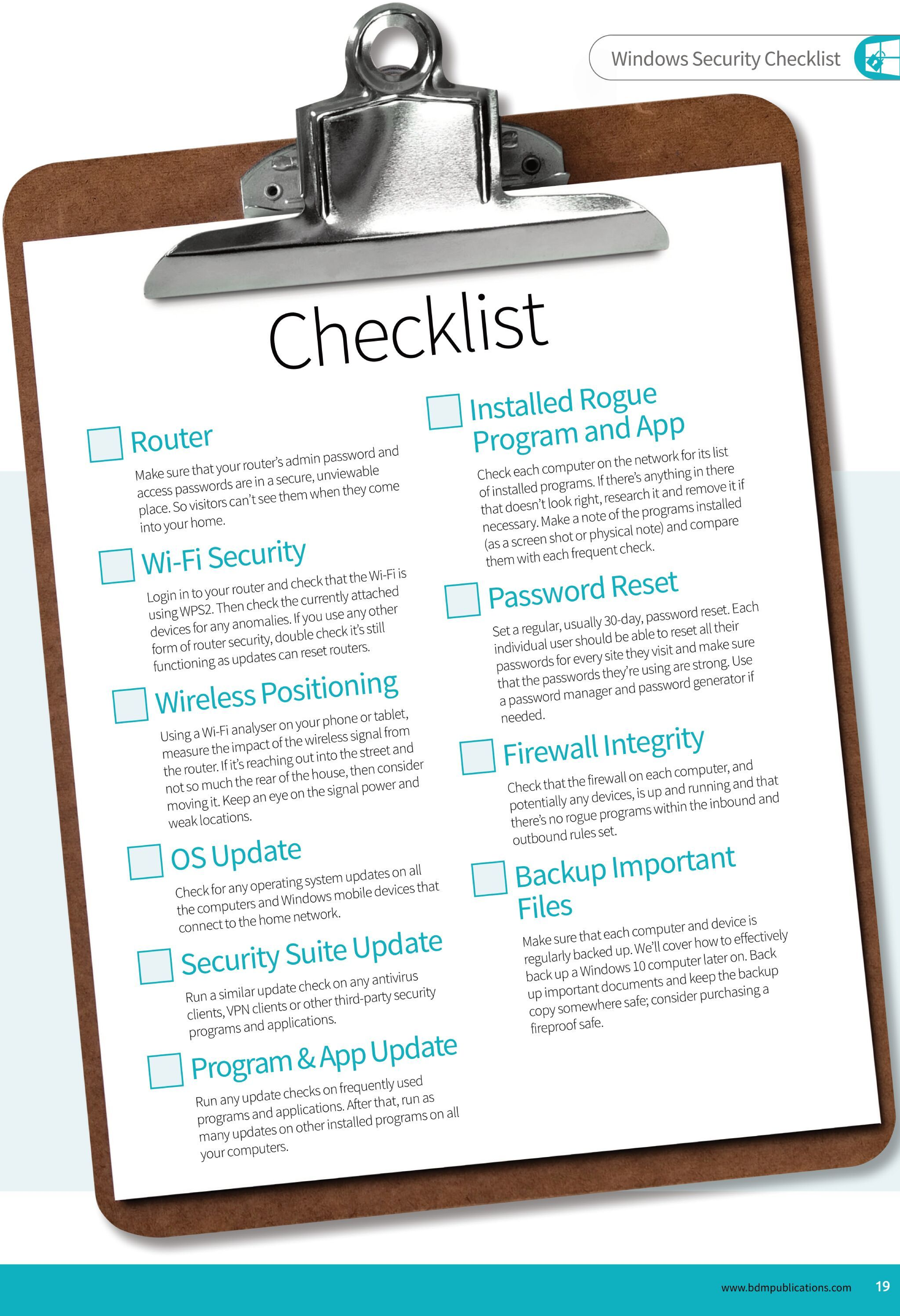
Windows Security Checklist

Taking the time to write down an effective security plan for your home network will pay dividends in the long run. With it you're able to spot potential leaks in security, secure your home network, Wi-Fi and powerline adapter technologies, and ensure digital peace of mind.

Naturally, this is just our example and will probably be different to your own setup and depending on the equipment you have available to you. For the sake of this publication we've taken a more generic approach but it's worth using it as a foundation from which you build your own, personal and unique checklist. Your checklist can be as intricate as you like, detailing specific hardware or software on one or all your computers, devices and so on, that needs to be updated regularly. Just remember though, there is a point where you can become a little too security conscious. Whilst it's great to be prepared for anything, and run your home network like a veritable digital Fort Knox, it can take up a substantial amount of your time applying patches and checking off every item on the list. Therefore, look for a happy medium, whilst remaining vigilant against digital threats.

We've come up with a template security checklist that you can use to create your own, for your home network. Remember to tick each section and remember to keep checking regularly and alter it as new devices are added.

> **Plan Ahead**



Checklist

☐ Router

Make sure that your router's admin password and access passwords are in a secure, unviewable place. So visitors can't see them when they come into your home.

☐ Wi-Fi Security

Login in to your router and check that the Wi-Fi is using WPS2. Then check the currently attached devices for any anomalies. If you use any other form of router security, double check it's still functioning as updates can reset routers.

☐ Wireless Positioning

Using a Wi-Fi analyser on your phone or tablet, measure the impact of the wireless signal from the router. If it's reaching out into the street and not so much the rear of the house, then consider moving it. Keep an eye on the signal power and weak locations.

☐ OS Update

Check for any operating system updates on all the computers and Windows mobile devices that connect to the home network.

☐ Security Suite Update

Run a similar update check on any antivirus clients, VPN clients or other third-party security programs and applications.

☐ Program & App Update

Run any update checks on frequently used programs and applications. After that, run as many updates on other installed programs on all your computers.

☐ Installed Rogue Program and App

Check each computer on the network for its list of installed programs. If there's anything in there that doesn't look right, research it and remove it if necessary. Make a note of the programs installed (as a screen shot or physical note) and compare them with each frequent check.

☐ Password Reset

Set a regular, usually 30-day, password reset. Each individual user should be able to reset all their passwords for every site they visit and make sure that the passwords they're using are strong. Use a password manager and password generator if needed.

☐ Firewall Integrity

Check that the firewall on each computer, and potentially any devices, is up and running and that there's no rogue programs within the inbound and outbound rules set.

☐ Backup Important Files

Make sure that each computer and device is regularly backed up. We'll cover how to effectively back up a Windows 10 computer later on. Back up important documents and keep the backup copy somewhere safe; consider purchasing a fireproof safe.

What is a Sandbox?

Sandboxing is an important security technique that's used by companies and individuals the world over. It's not something the average user will normally come across but you can guarantee that every piece of software you use has been sandboxed at some point in its development.

Playing in the Sand

Everyone from software developers and security experts to the hackers themselves will use a sandbox environment to help build and test their products; so what exactly is a sandbox?

Just as the name suggests, a sandbox is a place where you can do something without it affecting the surrounding area: visualise a sandbox in the middle of a garden. In digital security terms, this means a sandbox is a tightly controlled environment that's isolated from the main operating system where a person can test or analyse software and its impact on a virtual system.

The sandbox can be one of a number of implementations: web based, operating system based, program based, network based or even emulating interaction with the Internet. There are countless more examples, each depending on what exactly is being tested and what functions are required to complete the test.

For security, a sandbox is usually an extremely isolated environment that doesn't have access to anything on the company network, or any contact with a host machine. Here the security expert is able to conducts tests on untrusted pieces of code, known malware and viruses and even website content. Should those tests reveal something nasty within, the security expert is able to work their magic and develop a fix that can be further tested and finally deployed to the company's servers, where it's downloaded as updated virus definitions by the security suites and applied to a customer's computer.

Imagine that from the point of view of a hacker, then. The hacker has developed a particularly nasty piece of code that could bring down government agencies and cause widespread panic among the global digital community; they're hardly going to test it on their own computer. They need to create a sandbox environment whereby they can trigger the malware, ransomware or whatever, and let it run its course. In the meantime they can run through various procedures to try and wipe the malware, as a security expert would, to find any weaknesses. Once they've perfected the malware and wiped out any perceivable vulnerabilities, they can then happily upload it to the Internet and sit back as the world is infected with their code.

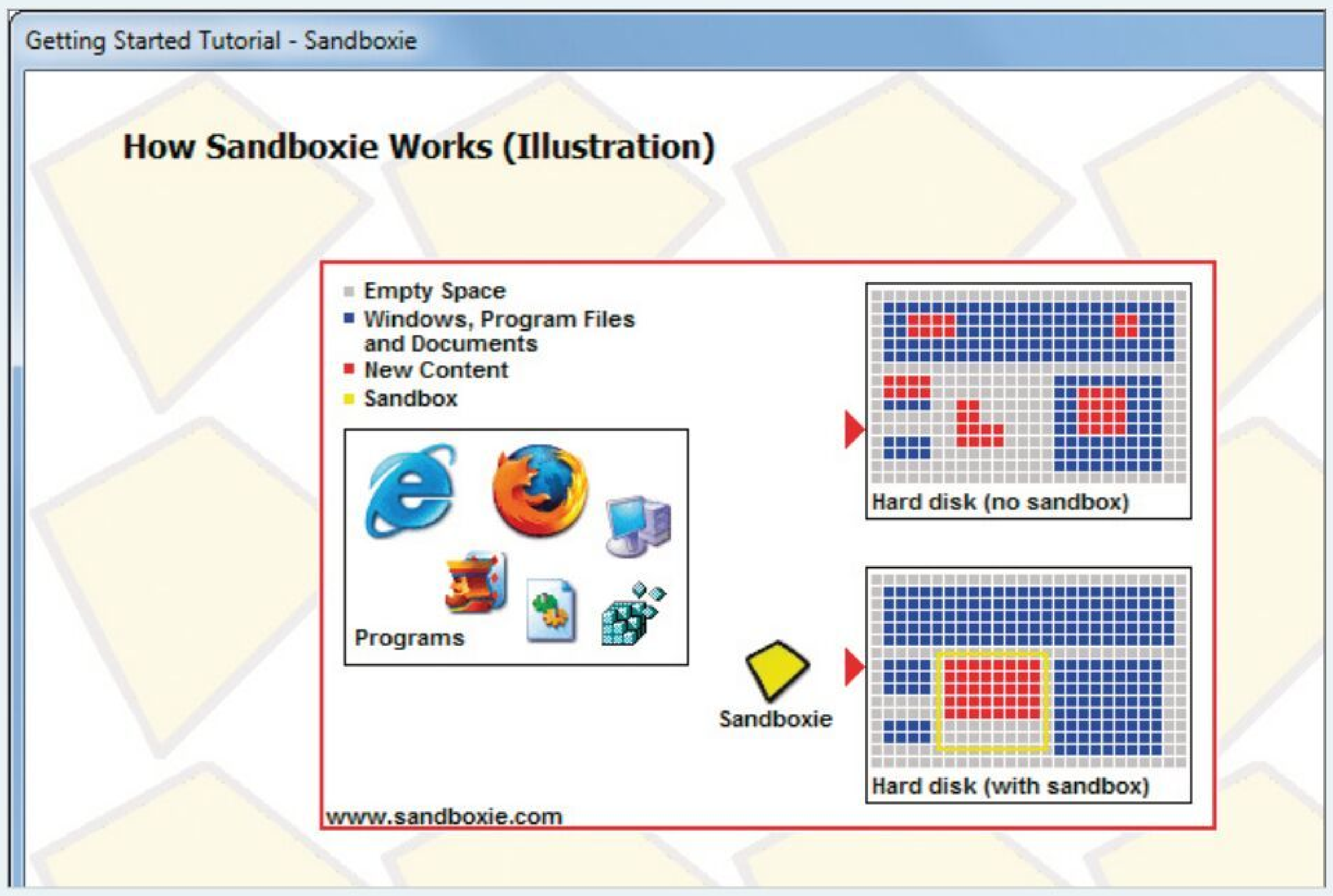
It's not always the testing of malicious code that's associated with sandboxes. For example, the words you're reading now were written using Office 365/Word 2016. Before the product was released by Microsoft, the development team behind Word will have gone through extensive testing, making sure that all the individual components within and that make up Word 2016 all worked. To do so, they will have used a dedicated and separate environment to the one they're using to program on. This specialised environment will have mimicked a real world setup as much as possible, so that when the developer wanted to test something they could compile the code and execute it in an environment that wouldn't affect their normal day-to-day workplace.

The often severe lockdown of a sandbox system does make it difficult to emulate what the average user may be using. The standard desktop computer has many different elements, both hardware and software, that work together to make up the computer that you've customised and personalised. A developer, security expert or software tester can never hope to create something that works 100 percent with every Windows 10 desktop system that's out there.

It's generally accepted then that when testing in a sandbox it's advisable to use as common a hardware and software setup as possible. This way, the developer will likely create a program that works on as high percentage of the computers available. Those computers that differ from the norm, and that may require a little more work for the product to install and work on, can then be dealt with through minor patching and bug testing.

So what's this got to do with you, we hear you say. Well, there are ways in which you can create your own sandbox environment to test in. Consider how many times you've downloaded software from the Internet and executed it without even examining how it may affect your computer. How many times do you visit websites and happily click on whatever message may appear without even reading it properly. With your own sandbox environment, you can download and install a piece of software and see how it runs within a test setup without it ever impacting your real machine. If you get into the habit of testing every bit of software in a sandbox first, you'll certainly be glad should the day come you discover a hidden virus in the folds of an otherwise harmless looking program.

> *Using a virtual machine as a sandbox is a great way to test programs for every version of Windows, not just the latest*


Getting Started Tutorial - Sandboxie
How Sandboxie Works (Illustration)
Empty Space
Windows, Program Files and Documents
New Content
Sandbox
Programs
Sandboxie
Hard disk (no sandbox)
Hard disk (with sandbox)
www.sandboxie.com

"Sandboxie is an environment designed to allow you to test programs without them being installed on your computer."

VirtualBox

"VirtualBox is considered to be one of the leading and easiest to use virtual machines, where you can create a sandbox environment to test in."

Running Windows 10 as a Sandbox

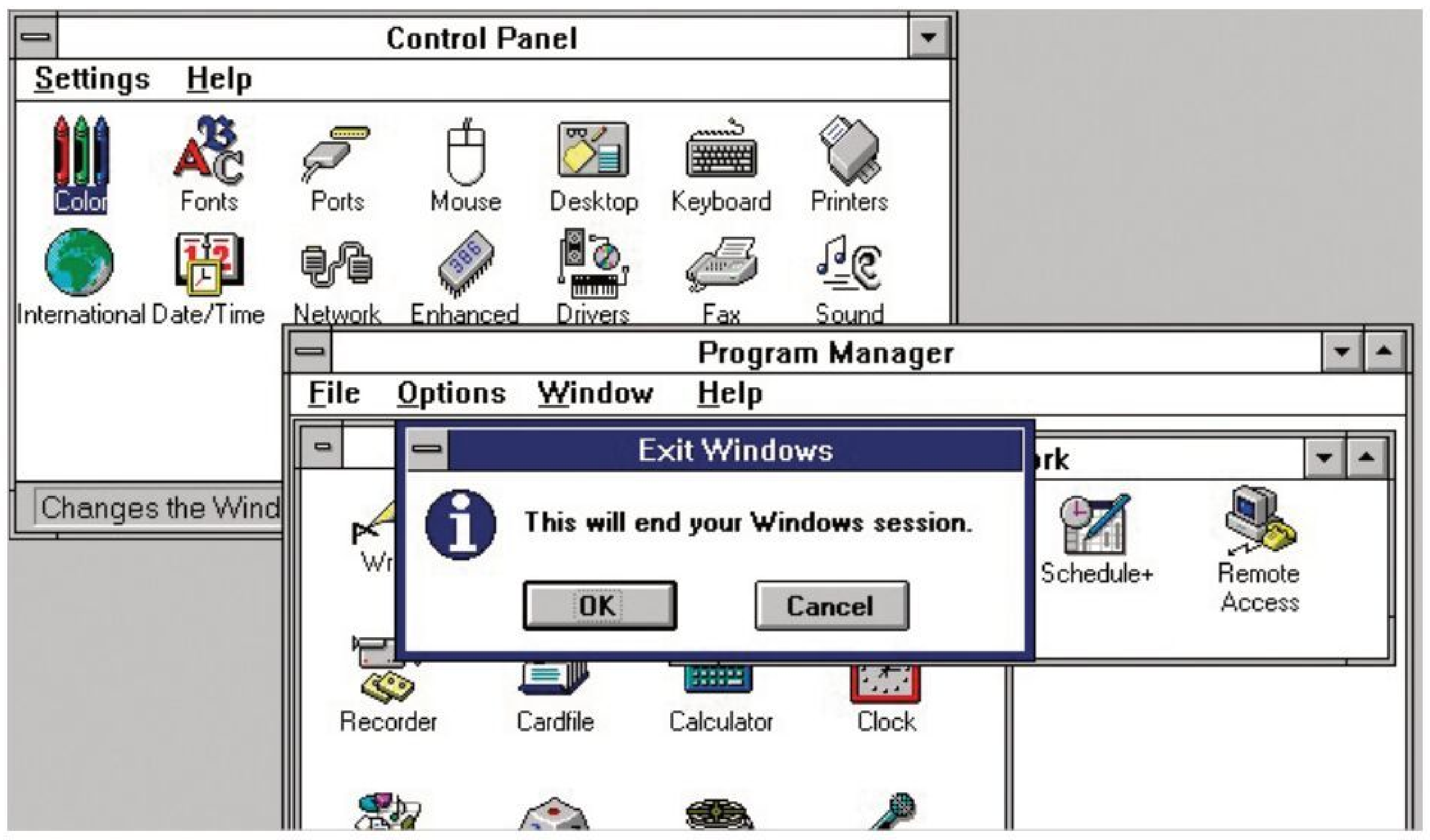
We've already talked about how a sandbox works and essentially what one is in terms of computing and security. However there are many advantages to creating your own virtual sandbox environment. It's not always purely to test suspicious code, as you'll soon discover.

Sand Between Your Toes

If you're still convinced that a sandbox environment can help you out, then read on. We've compiled a list of ten reasons why creating your own Windows 10 sandbox is beneficial to the average user.

OLD PROGRAMS

Within the Windows 10 virtual sandbox environment you may be able to run older programs that would normally fail, even in compatibility mode, under more modern hardware drivers. Often an older program will look for a specific driver set, if it's too modern then it can fail. Virtual environments use older type drivers by default.


Control Panel
Settings Help
Color
Fonts
Ports
Mouse
Desktop
Keyboard
Printers
International
Date/Time
Network
Enhanced
Drivers
Fax
Sound
Changes the Wind
Program Manager
File Options Window Help
Exit Windows
OK
Cancel
Schedule+
Remote Access
Recorder
Cardfile
Calculator
Clock

This will end your Windows session.

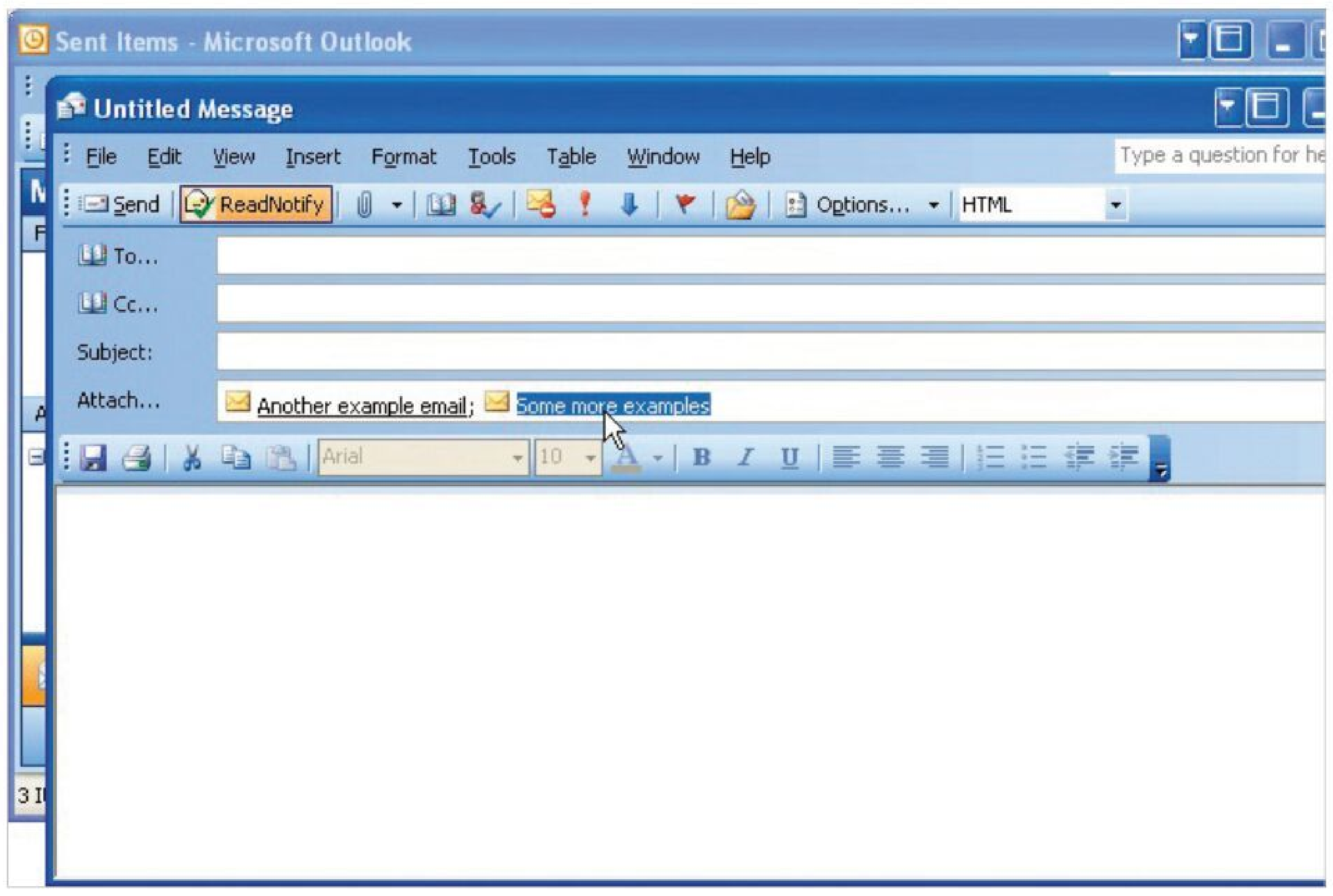
SAFE BROWSING

Within a virtual environment you can browse a site without any of its code being written to the main, host computer. This could simply be cookies and other such relatively harmless additions to sites or it could include data miners and malicious links.

The Million Dollar Homepage
1,000,000 pixels • $1 per pixel • Own a piece of internet history!
SOLD OUT!

HOST PROTECTION

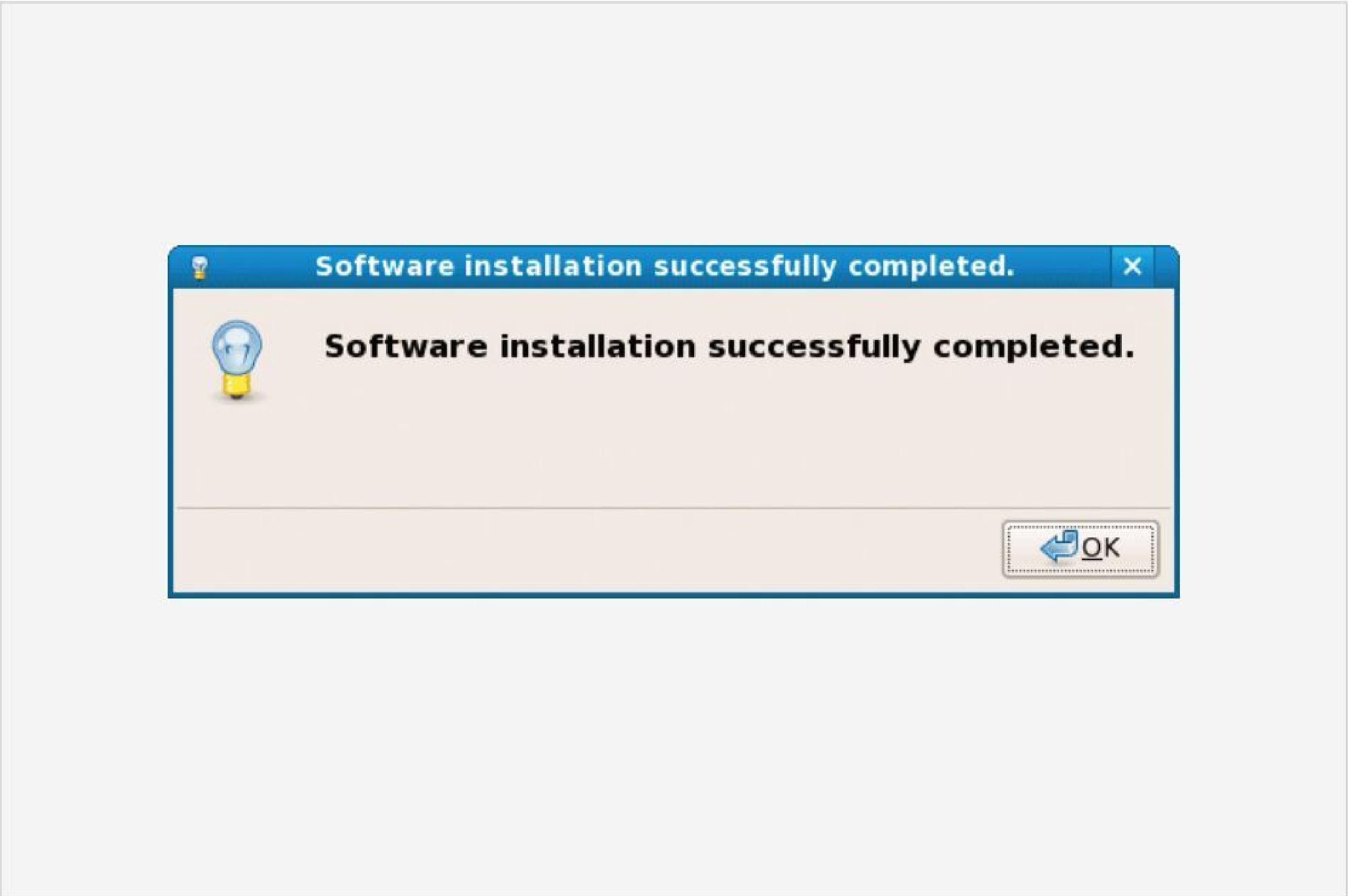
If you think that a download link or email attachment may contain a virus, then opening it in a safe, virtual environment is the safest bet. Of course, you shouldn't open any unknown email attachments but if you need to, do so in a sandbox. The virus will infect the sandbox and not the host (real) computer.


Sent Items - Microsoft Outlook
Untitled Message
File Edit View Insert Format Tools Table Window Help
Type a question for he
Send
ReadNotify
Options...
HTML
To...
Cc...
Subject:
Attach...
Arial
10
B I U

Attach... Another example email; Some more examples

SOFTWARE TESTING

If you're serious about your security and the safety of your home computer, then you should be downloading and installing software in a test environment first before applying it to your real computer. A virtual environment is a great place to see how software works and whether it's worth installing or not.

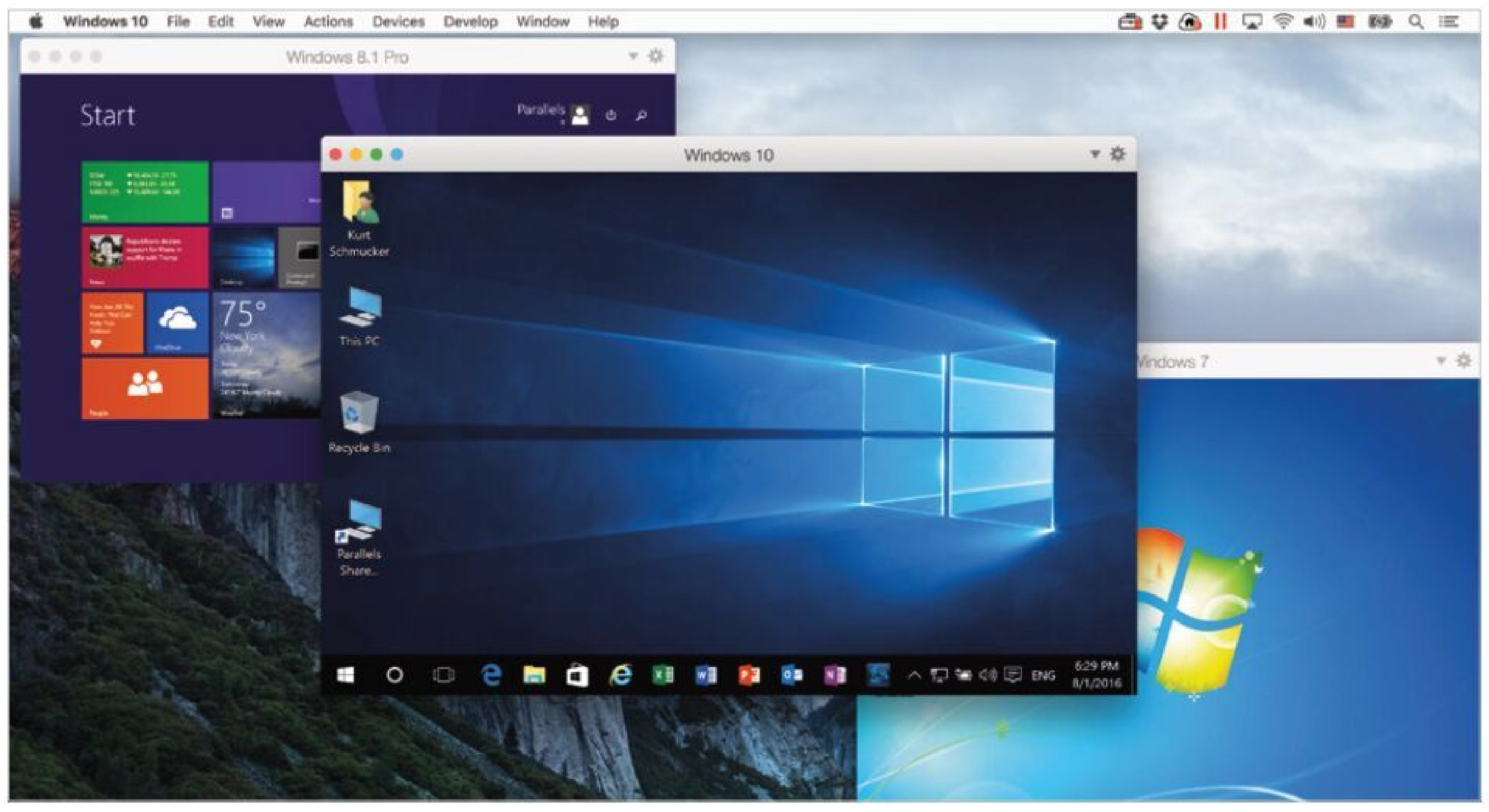


Software installation successfully completed.

Software installation successfully completed.

VIRTUAL OS

The beauty of a virtual environment, such as one created by VirtualBox, is that you're able to run Windows, macOS and Linux operating systems on top of your host operating system, whatever system that may be. You can install Windows 10 within a virtual environment whilst using Linux or macOS, or vice versa.

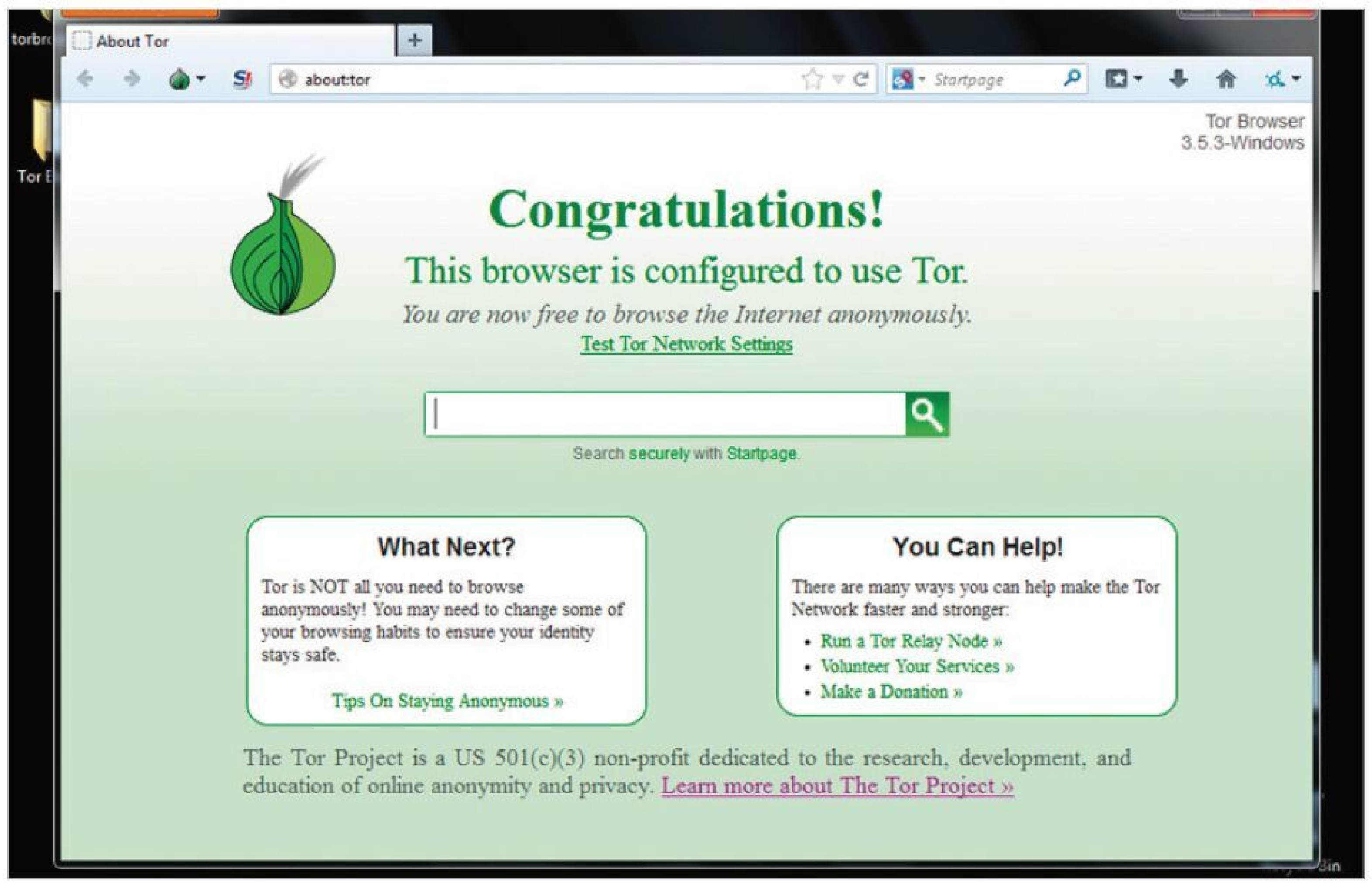


VIRTUAL BACKUP

It is possible to create a virtual copy of a physical machine. This is an excellent way of making sure that the entire machine, that is a snapshot of the OS as it was when copied, is safely backed up and accessible regardless of what operating system you choose to use.

SECURE ANONYMITY

Within a virtual Windows 10 environment you're able to create an anonymity system. By this we mean, you can install a VPN and use the Tor network and surf the Internet without fear of being traced; and what's more, none of it will affect your host operating system.



Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

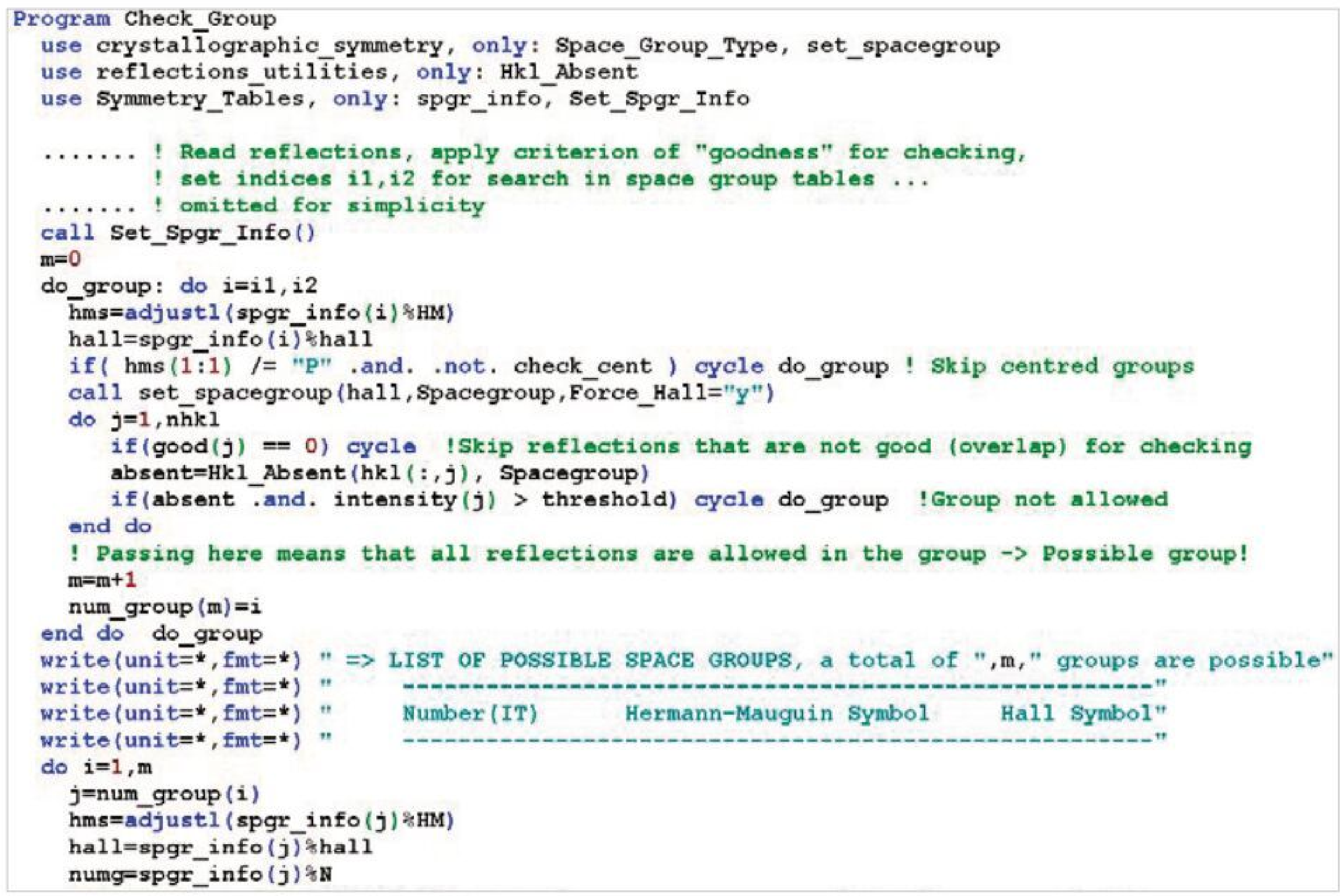
There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

SAFE DEVELOPMENT

If you're considering developing your own software and apps, then using a virtual environment is an ideal place to test the code as you create it. Should a function you've written have an adverse effect on the OS, then you won't damage your working system.



```
Program Check_Group
  use crystallographic_symmetry, only: Space_Group_Type, set_spacegroup
  use reflections_utilities, only: Hkl_Absent
  use Symmetry_Tables, only: spgr_info, Set_Spgr_Info

  ....... ! Read reflections, apply criterion of "goodness" for checking,
          ! set indices i1,i2 for search in space group tables ...
  ....... ! omitted for simplicity
  call Set_Spgr_Info()
  m=0
  do_group: do i=i1,i2
    hms=adjustl(spgr_info(i)%HM)
    hall=spgr_info(i)%hall
    if( hms(1:1) /= "P" .and. .not. check_cent ) cycle do_group ! Skip centred groups
    call set_spacegroup(hall,Spacegroup,Force_Hall="y")
    do j=1,nhkl
       if(good(j) == 0) cycle  !Skip reflections that are not good (overlap) for checking
       absent=Hkl_Absent(hkl(:,j), Spacegroup)
       if(absent .and. intensity(j) > threshold) cycle do_group  !Group not allowed
    end do
    ! Passing here means that all reflections are allowed in the group -> Possible group!
    m=m+1
    num_group(m)=i
  end do  do_group
  write(unit=*,fmt=*) " => LIST OF POSSIBLE SPACE GROUPS, a total of ",m," groups are possible"
  write(unit=*,fmt=*) "     ------------------------------------------------------------"
  write(unit=*,fmt=*) "     Number(IT)      Hermann-Mauguin Symbol     Hall Symbol"
  write(unit=*,fmt=*) "     ------------------------------------------------------------"
  do i=1,m
    j=num_group(i)
    hms=adjustl(spgr_info(j)%HM)
    hall=spgr_info(j)%hall
    numg=spgr_info(j)%N
```

FAMILY FRIENDLY

If you have a single-family computer, a virtual environment is a great place for the kids to go without fear of them potentially breaking the system. It doesn't happen often, kids are mostly more tech-savvy than adults but little fingers do have a habit of clicking things they're not supposed to. Virtual environments can be backed up and redeployed easily.

RESTRICTED ACCOUNTS

Again, using children as an example, a virtual child's Windows 10 account can come with all manner of restrictions and monitoring software, to stop them from wandering into the scarier parts of the Internet, such as installing Net Nanny. Again, these controls won't affect the host computer or adult accounts.

Net Nanny

18+

WHAT IS
AVAXHOME?

AVAXHOME -

the biggest Internet portal, providing you various content: brand new books, trending movies, fresh magazines, hot games, recent software, latest music releases.

Unlimited satisfaction one low price
Cheap constant access to piping hot media
Protect your downloadings from Big brother
Safer, than torrent-trackers

18 years of seamless operation and our users' satisfaction

All languages
Brand new content
One site

AVXLIVE.ICU

AvaxHome - Your End Place

We have everything for all of your needs. Just open https://avxlive.icu

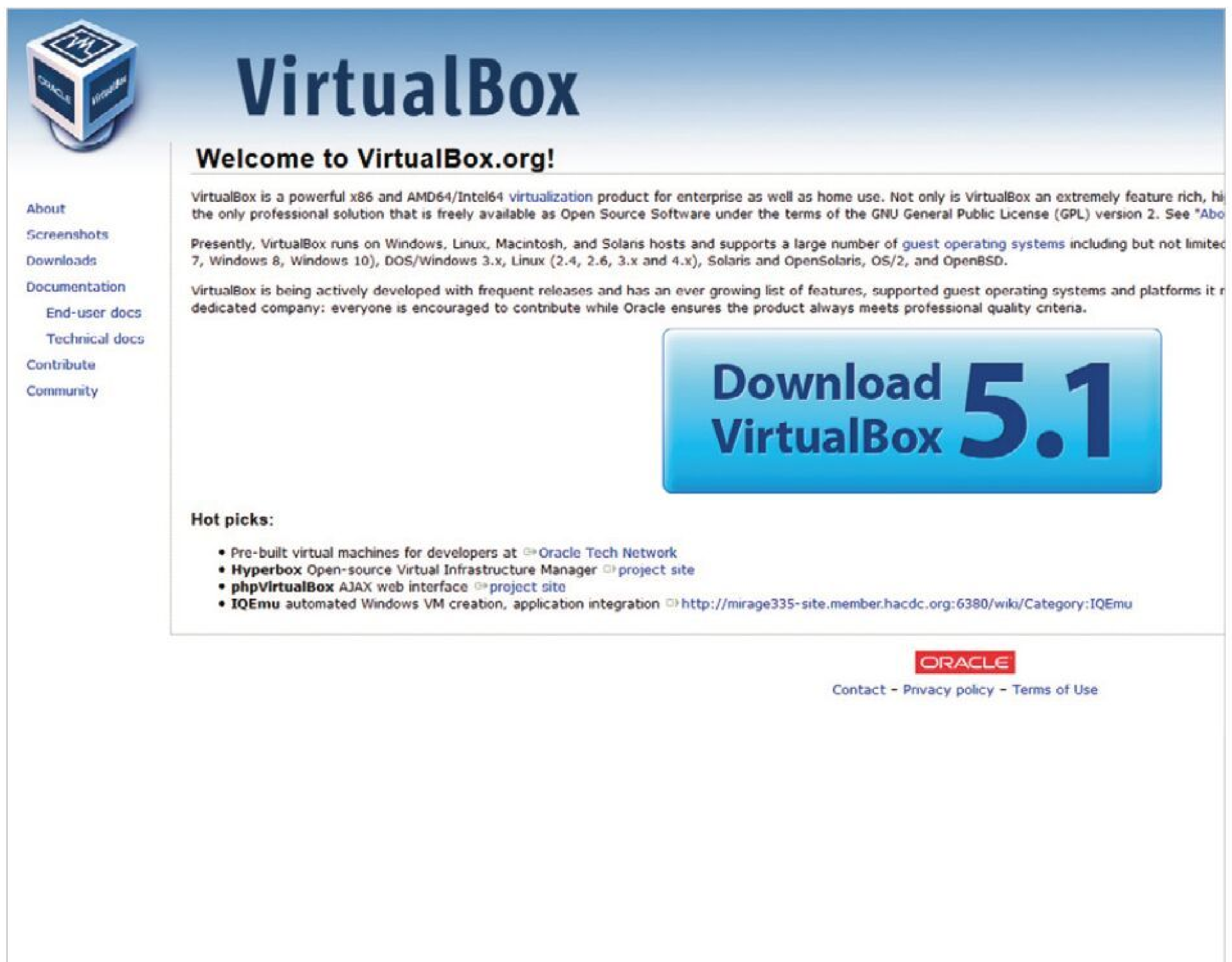
Installing VirtualBox

Oracle's VirtualBox is one of the easiest virtual machine platforms for the beginner to experiment on. Within it you can install Windows, Linux and even macOS for sandbox testing, without ever having to alter your main computer's setup.

Going Virtual

Using a Virtual Machine (VM) will take resources from your computer: memory, hard drive space, processor usage and so on. So make sure you have enough of each before commencing.

STEP 1 The first task is getting hold of VirtualBox. If you haven't already, head over to www.virtualbox.org and click on the large 'Download VirtualBox 5.1' box. This will take you to the main download page. Locate the correct host for your system, Windows or Mac, the Host is the current installed, main operating system, and click to begin the download.



Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, hi
the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. See "Abo

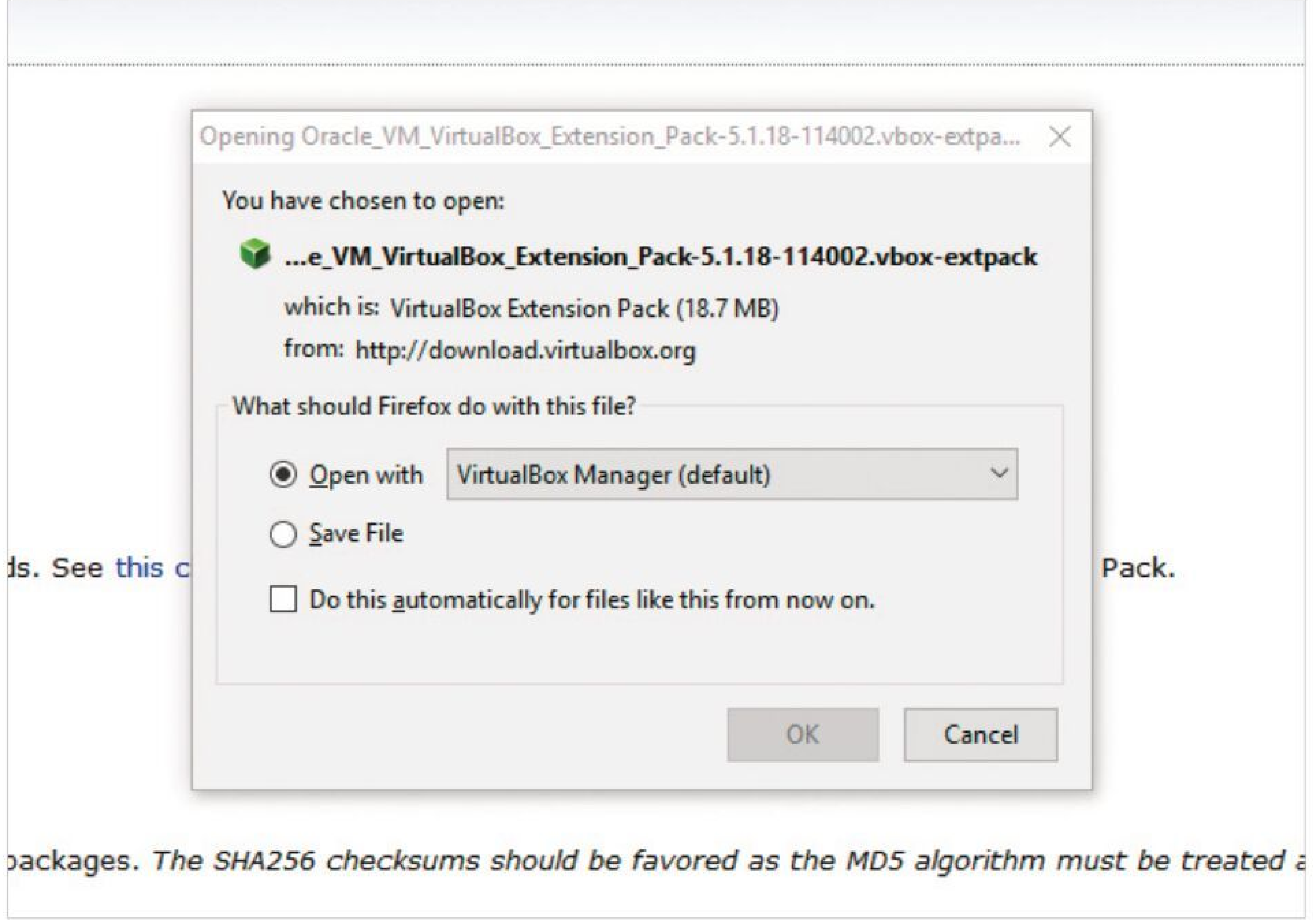
Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limitec
7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it r
dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

Hot picks:

- Pre-built virtual machines for developers at Oracle Tech Network
- **Hyperbox** Open-source Virtual Infrastructure Manager project site
- **phpVirtualBox** AJAX web interface project site
- **IQEmu** automated Windows VM creation, application integration http://mirage335-site.member.hacdc.org:6380/wiki/Category:IQEmu

STEP 2 Next, whilst still at the VirtualBox download page, locate the VirtualBox Extension Pack link. The Extension Pack supports USB devices, as well as numerous other extras that can help make the VM environment a more accurate emulation of a 'real' computer.



Opening Oracle_VM_VirtualBox_Extension_Pack-5.1.18-114002.vbox-extpa...

You have chosen to open:

...e_VM_VirtualBox_Extension_Pack-5.1.18-114002.vbox-extpack

which is: VirtualBox Extension Pack (18.7 MB)

from: http://download.virtualbox.org

What should Firefox do with this file?

● Open with VirtualBox Manager (default)

○ Save File

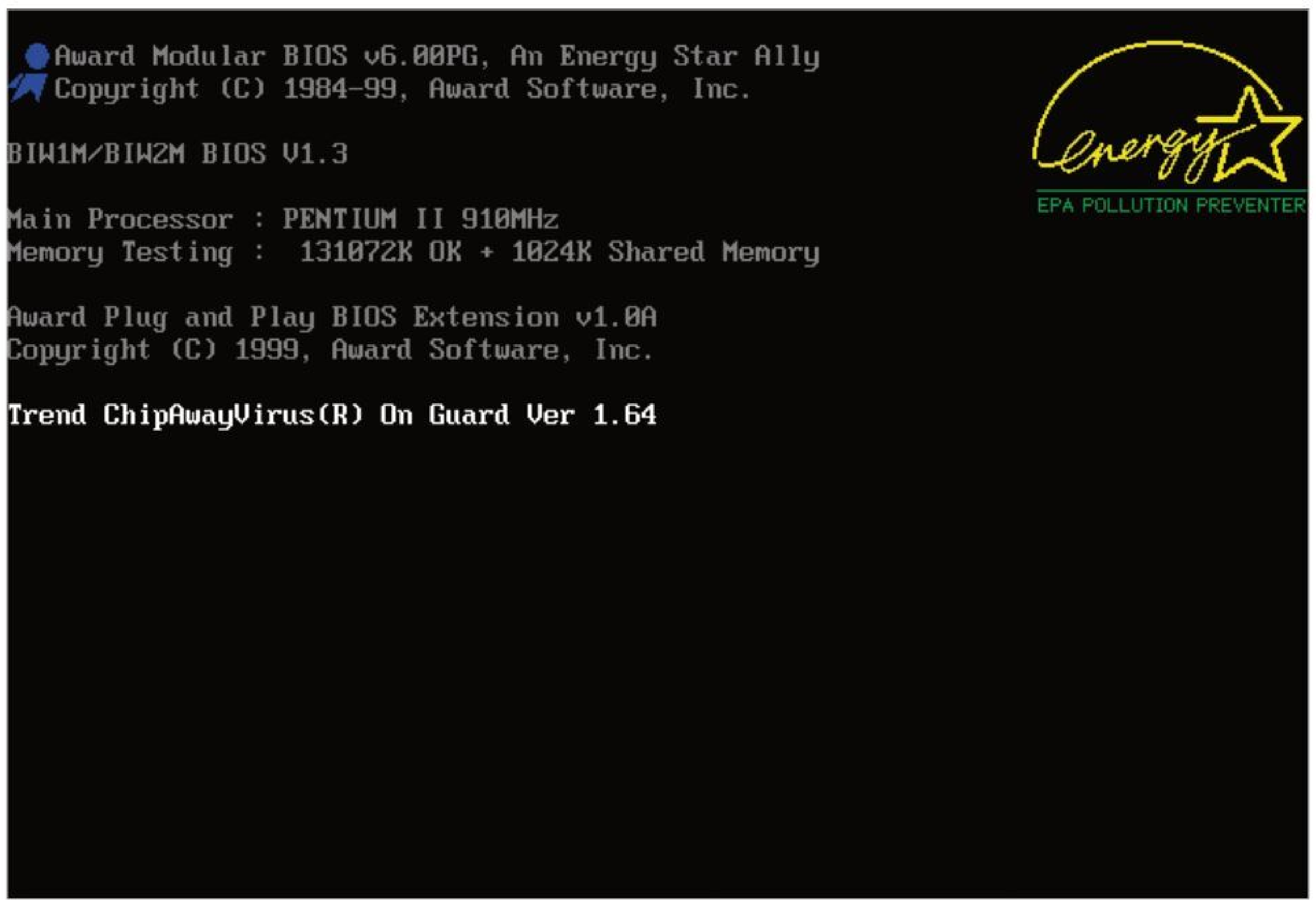
☐ Do this automatically for files like this from now on.

ds. See this c

Pack.

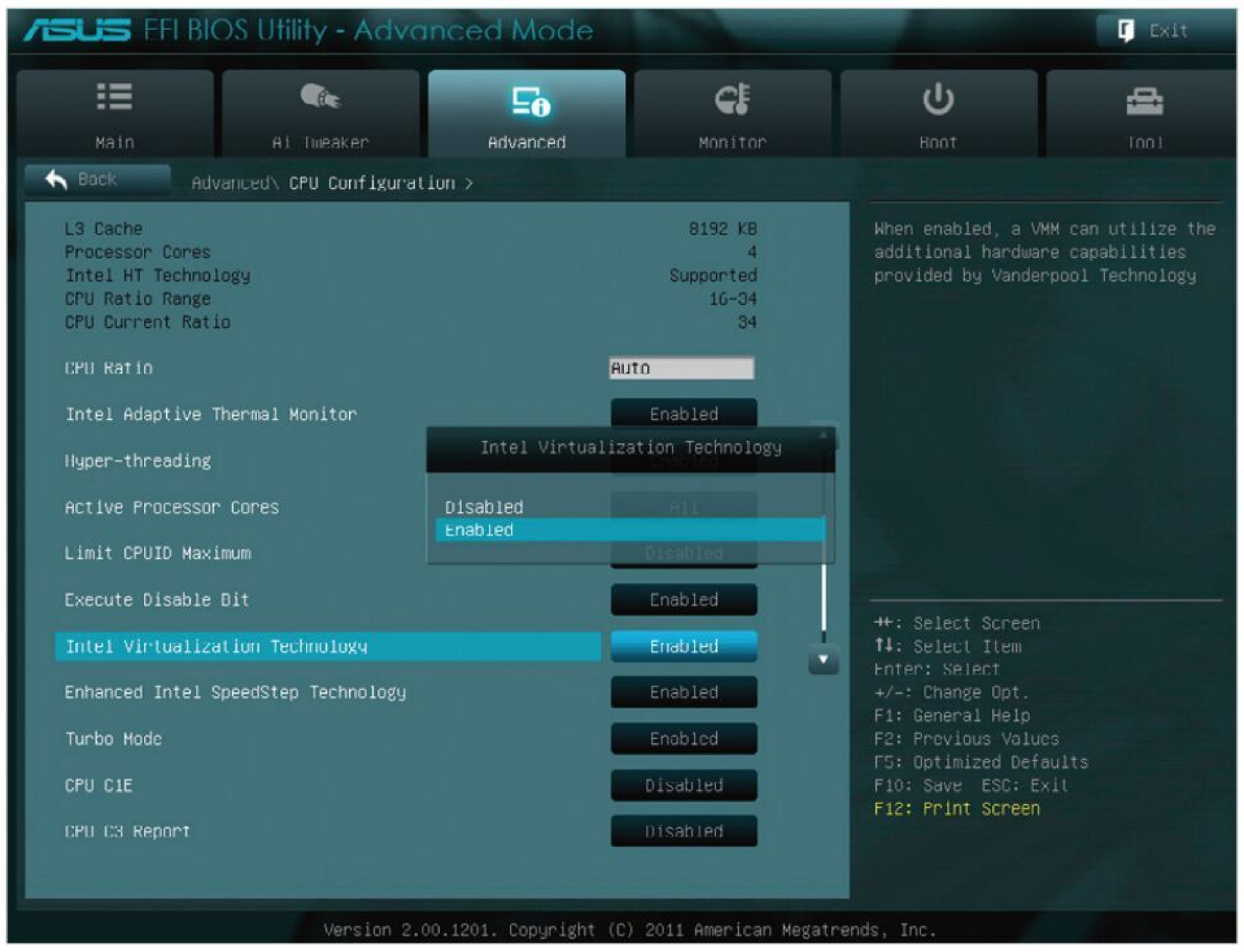
packages. The SHA256 checksums should be favored as the MD5 algorithm must be treated a

STEP 3 With the correct packages downloaded, and before you install anything, you need to make sure that the computer you're using is capable of hosting a VM. To do this, reboot the computer and enter the BIOS. When the computer starts up, press the Del, F2, or whichever key is necessary to Enter Setup.



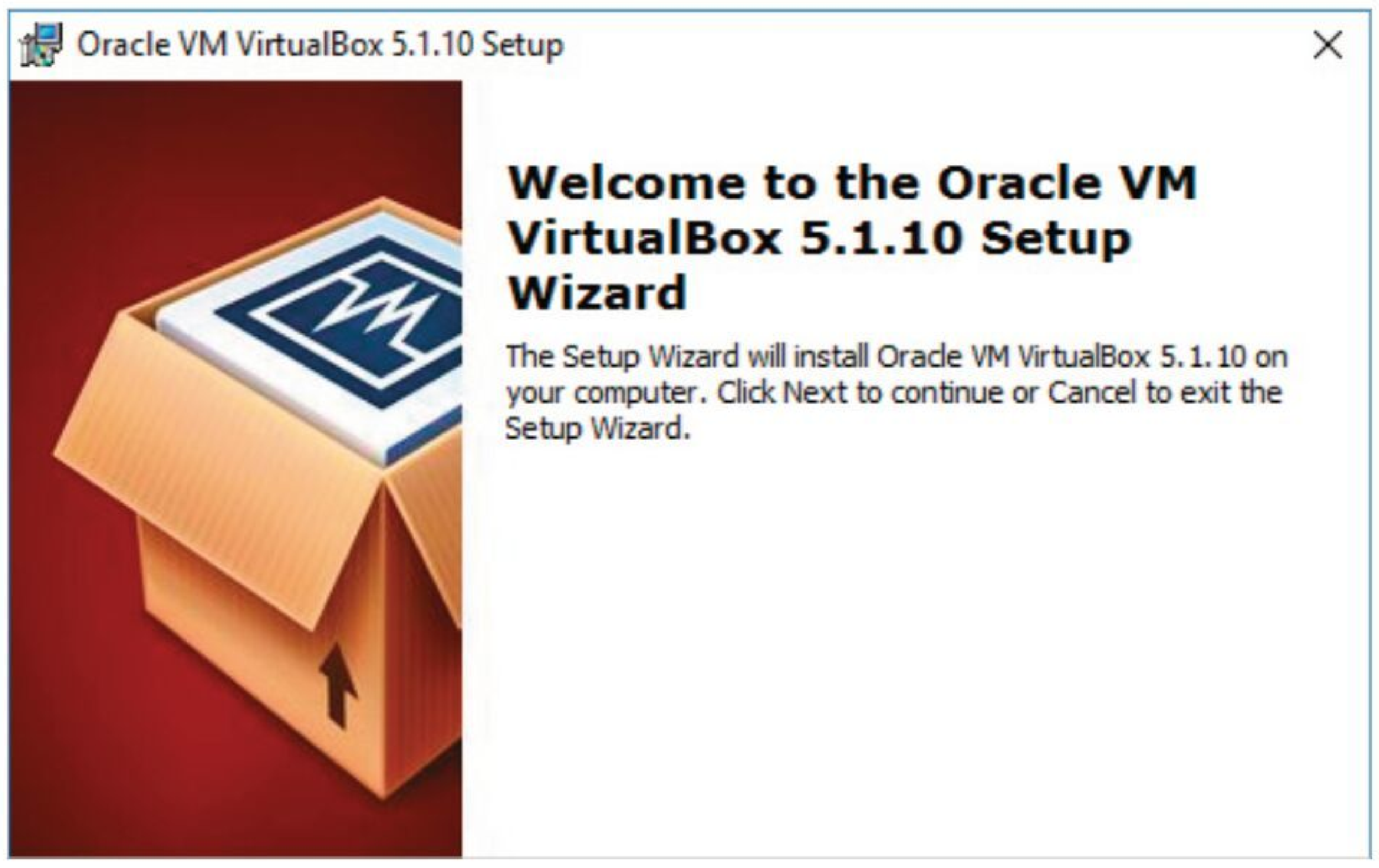
```
Award Modular BIOS v6.00PG, An Energy Star Ally
Copyright (C) 1984-99, Award Software, Inc.

BIW1M/BIW2M BIOS V1.3

Main Processor : PENTIUM II 910MHz
Memory Testing :  131072K OK + 1024K Shared Memory

Award Plug and Play BIOS Extension v1.0A
Copyright (C) 1999, Award Software, Inc.

Trend ChipAwayVirus(R) On Guard Ver 1.64
```

STEP 4 Each BIOS is laid out differently so it's very difficult to assess where to look in each personal example. However, as a general rule of thumb, you're looking for Intel Virtualisation Technology or simply Virtualisation: usually within the Advanced section of the BIOS. When you've located it, Enable it, save the settings, exit the BIOS and reboot the computer.



```
Advanced\ CPU Configuration >

L3 Cache                                    8192 KB
Processor Cores                                   4
Intel HT Technology                       Supported
CPU Ratio Range                               16-34
CPU Current Ratio                                34

CPU Ratio                                 Auto
Intel Adaptive Thermal Monitor            Enabled
Hyper-threading
Active Processor Cores
Limit CPUID Maximum
Execute Disable Bit                       Enabled
Intel Virtualization Technology           Enabled
Enhanced Intel SpeedStep Technology       Enabled
Turbo Mode                                Enabled
CPU C1E                                   Disabled
CPU C3 Report                             Disabled

        Intel Virtualization Technology
        Disabled
        Enabled

When enabled, a VMM can utilize the
additional hardware capabilities
provided by Vanderpool Technology

++: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F5: Optimized Defaults
F10: Save  ESC: Exit
F12: Print Screen

Version 2.00.1201. Copyright (C) 2011 American Megatrends, Inc.
```

STEP 5 With the computer back up and running, locate the downloaded main VirtualBox application and double-click to begin the installation process. Click Next to continue, when you're ready.

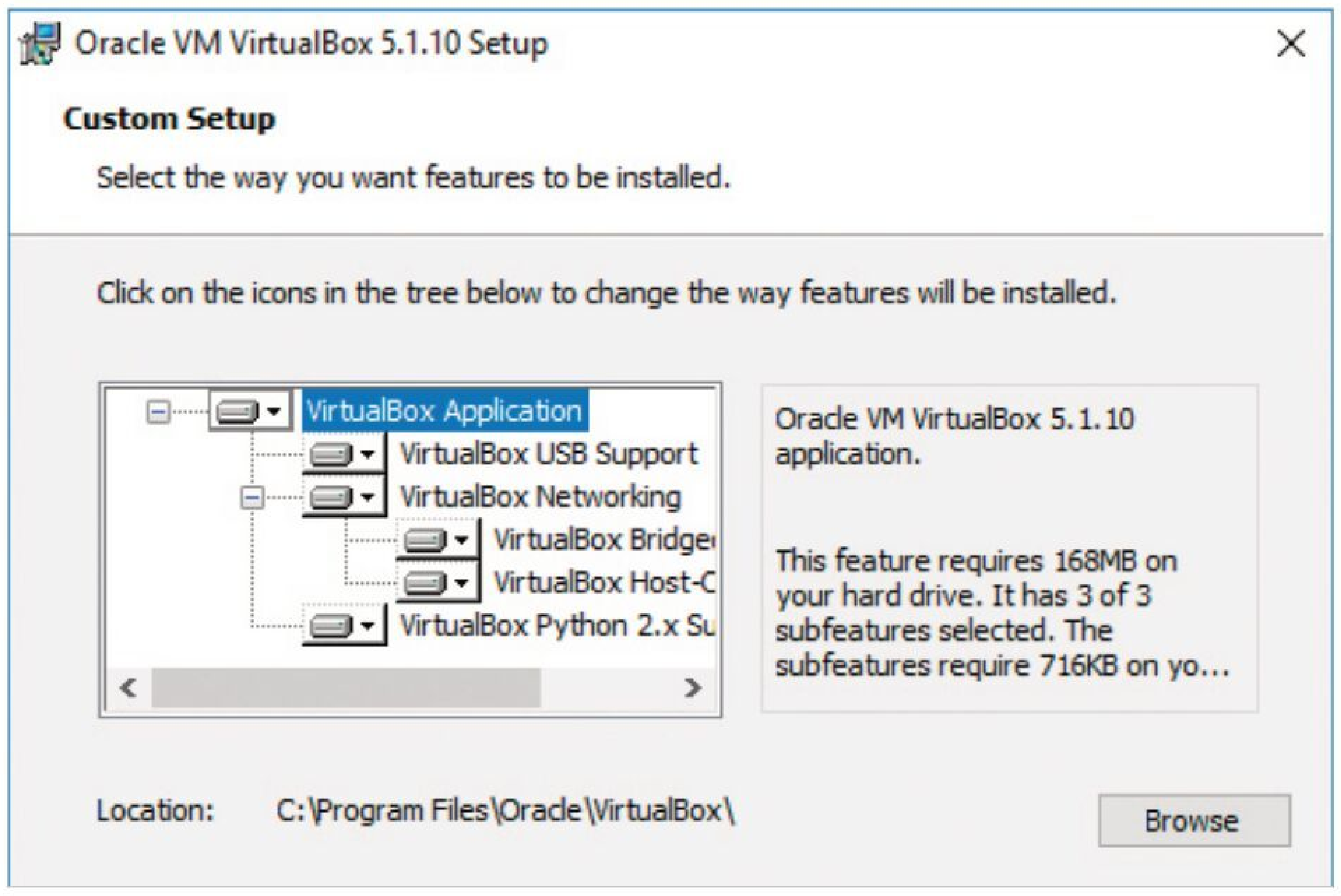


Oracle VM VirtualBox 5.1.10 Setup

Welcome to the Oracle VM VirtualBox 5.1.10 Setup Wizard

The Setup Wizard will install Oracle VM VirtualBox 5.1.10 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

STEP 6 The default installation location of VirtualBox should satisfy most users but if you have any special location requirements click on the 'Browse' button and change the install folder. Then, make sure that all the icons in the VirtualBox feature tree are selected and none of them has a red X next to them. Click Next to move on.



Oracle VM VirtualBox 5.1.10 Setup

Custom Setup

Select the way you want features to be installed.

Click on the icons in the tree below to change the way features will be installed.

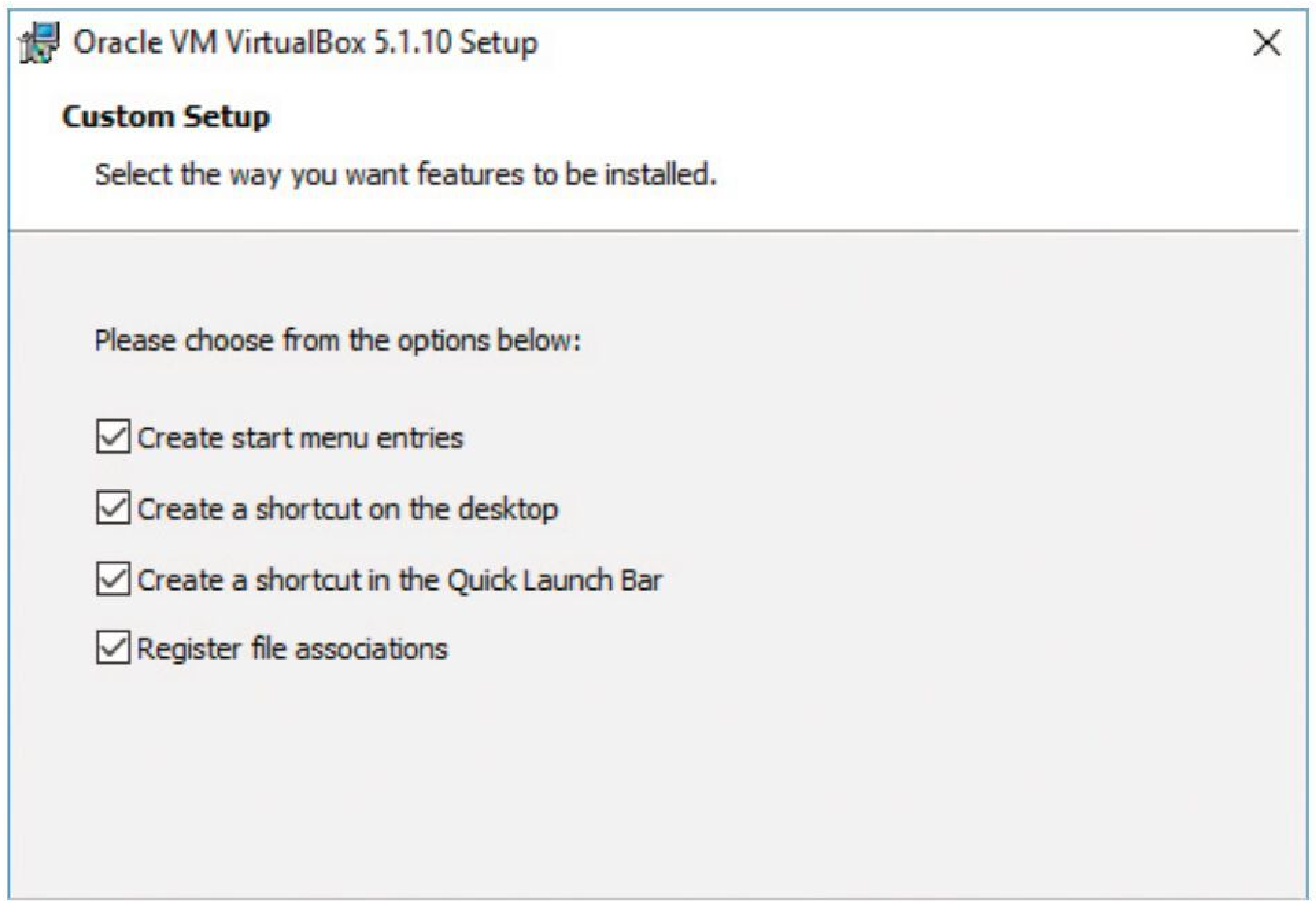
- VirtualBox Application
  - VirtualBox USB Support
  - VirtualBox Networking
    - VirtualBox Bridge
    - VirtualBox Host-C
  - VirtualBox Python 2.x Su

Oracle VM VirtualBox 5.1.10 application.

This feature requires 168MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 716KB on yo...

Location: C:\Program Files\Oracle\VirtualBox\

STEP 7 This section can be left alone to the defaults, should you wish. It simply makes life a little easier when dealing with VMs, especially when dealing with downloaded VMs, which you may encounter in the future. Again, clicking Next will move you on to the next stage.



Oracle VM VirtualBox 5.1.10 Setup

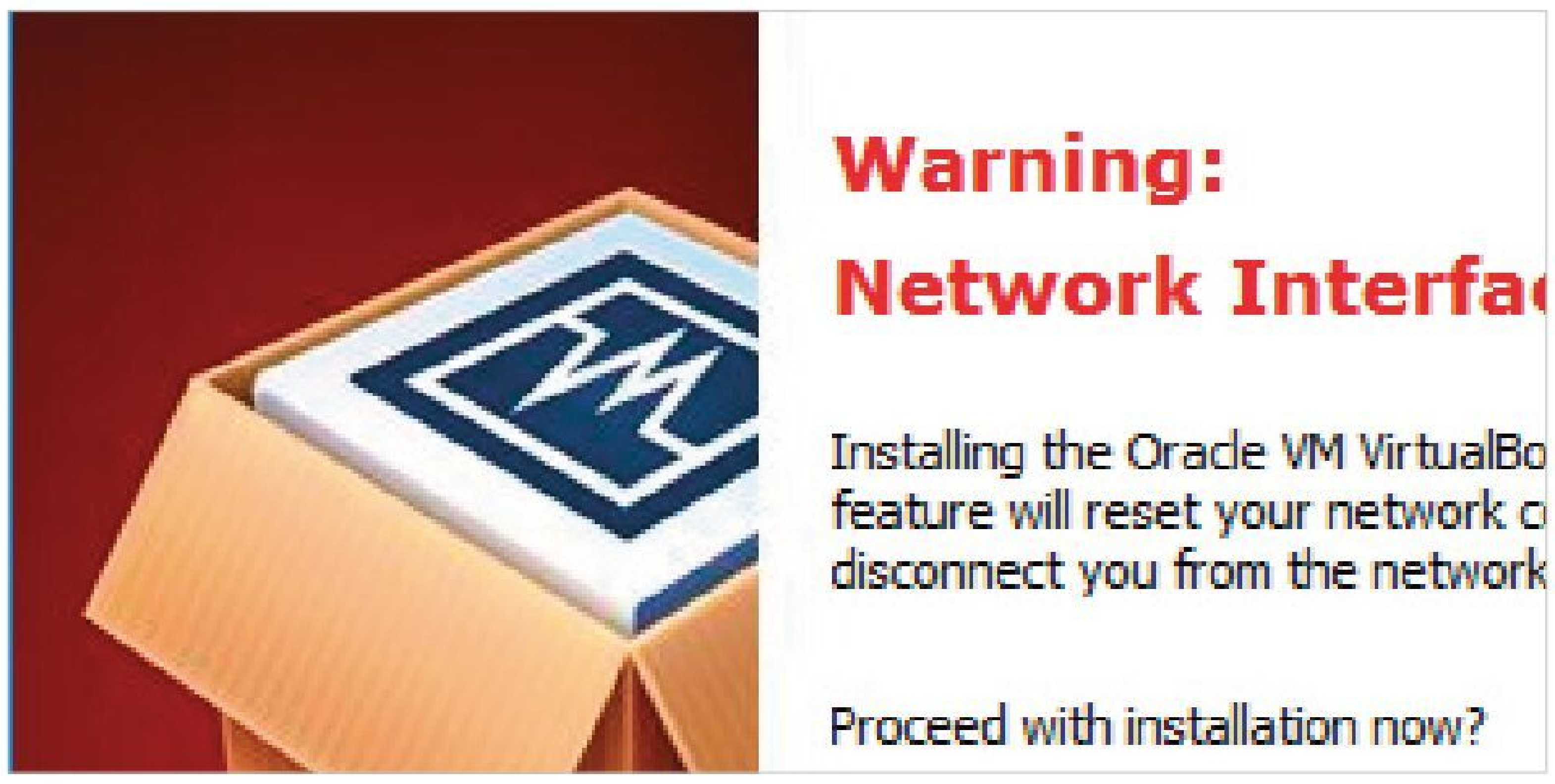
Custom Setup

Select the way you want features to be installed.

Please choose from the options below:

☑ Create start menu entries
☑ Create a shortcut on the desktop
☑ Create a shortcut in the Quick Launch Bar
☑ Register file associations

STEP 8 When installing VirtualBox your network connection will be disabled for a very brief period. This is due to VirtualBox creating a linked, virtual network connection so that any VM installed will be able to access the Internet, and your home network resources, via the computer's already established network connection. Click Yes, then Install to begin the installation.

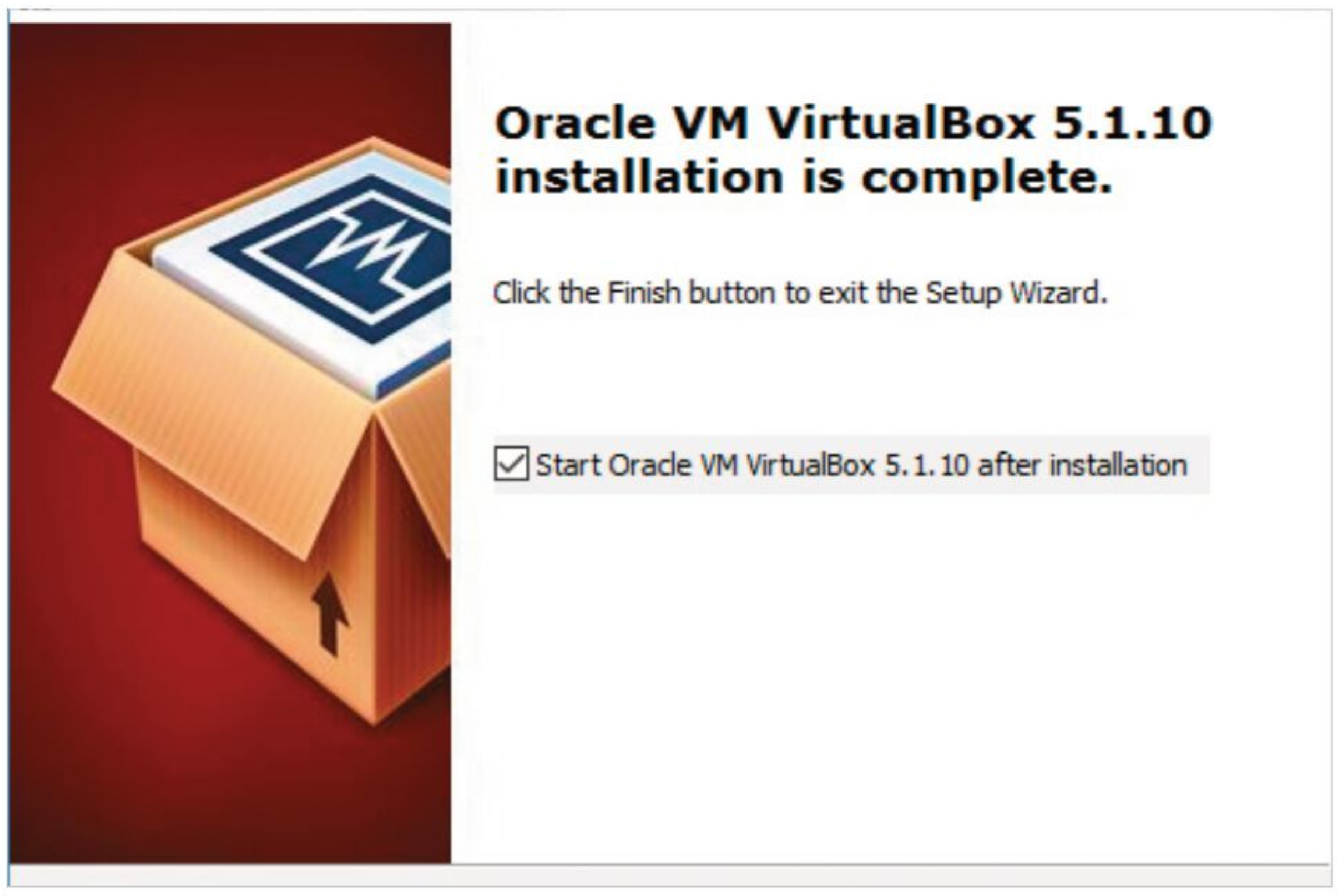


Warning: Network Interfa

Installing the Oracle VM VirtualBo
feature will reset your network c
disconnect you from the network

Proceed with installation now?

STEP 9 You may be asked by Windows to accept a security notification. Click Yes for this and you might encounter a dialogue box asking you to trust the installation from Oracle; again, click yes and accept the installation of the VirtualBox application. When it's complete, click Finish to start VirtualBox.

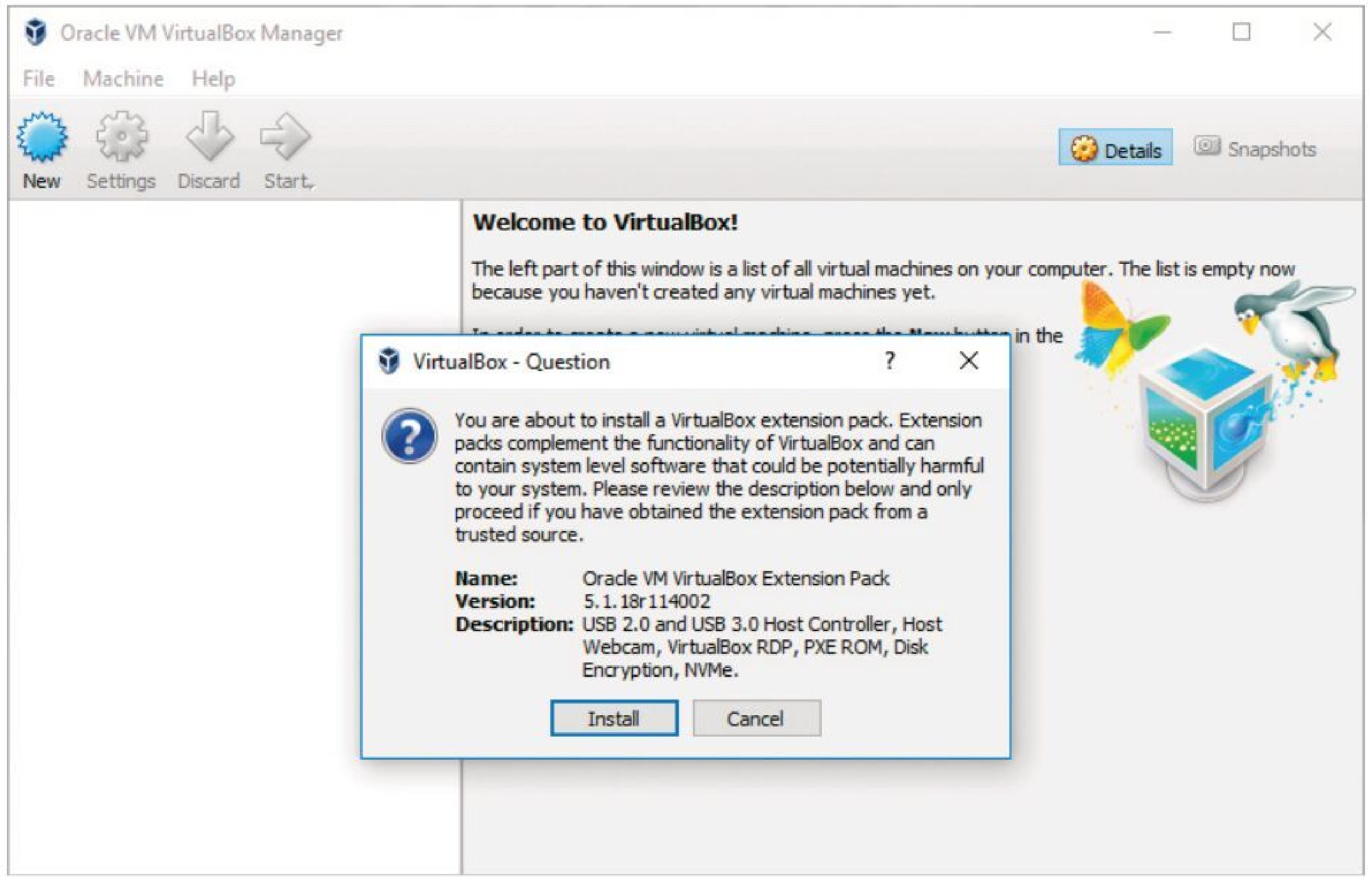


Oracle VM VirtualBox 5.1.10 installation is complete.

Click the Finish button to exit the Setup Wizard.

☑ Start Oracle VM VirtualBox 5.1.10 after installation

STEP 10 With VirtualBox up and running you can now install the VirtualBox Extension Pack. Locate the downloaded add-on and double-click. There may be a short pause whilst VirtualBox analyses the pack but you eventually receive a message to install it; obviously click Install to begin the process, scroll down the next screen to accept the agreement and click I Agree.



Oracle VM VirtualBox Manager

Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

VirtualBox - Question

You are about to install a VirtualBox extension pack. Extension packs complement the functionality of VirtualBox and can contain system level software that could be potentially harmful to your system. Please review the description below and only proceed if you have obtained the extension pack from a trusted source.

Name: Oracle VM VirtualBox Extension Pack
Version: 5.1.18r114002
Description: USB 2.0 and USB 3.0 Host Controller, Host Webcam, VirtualBox RDP, PXE ROM, Disk Encryption, NVMe.

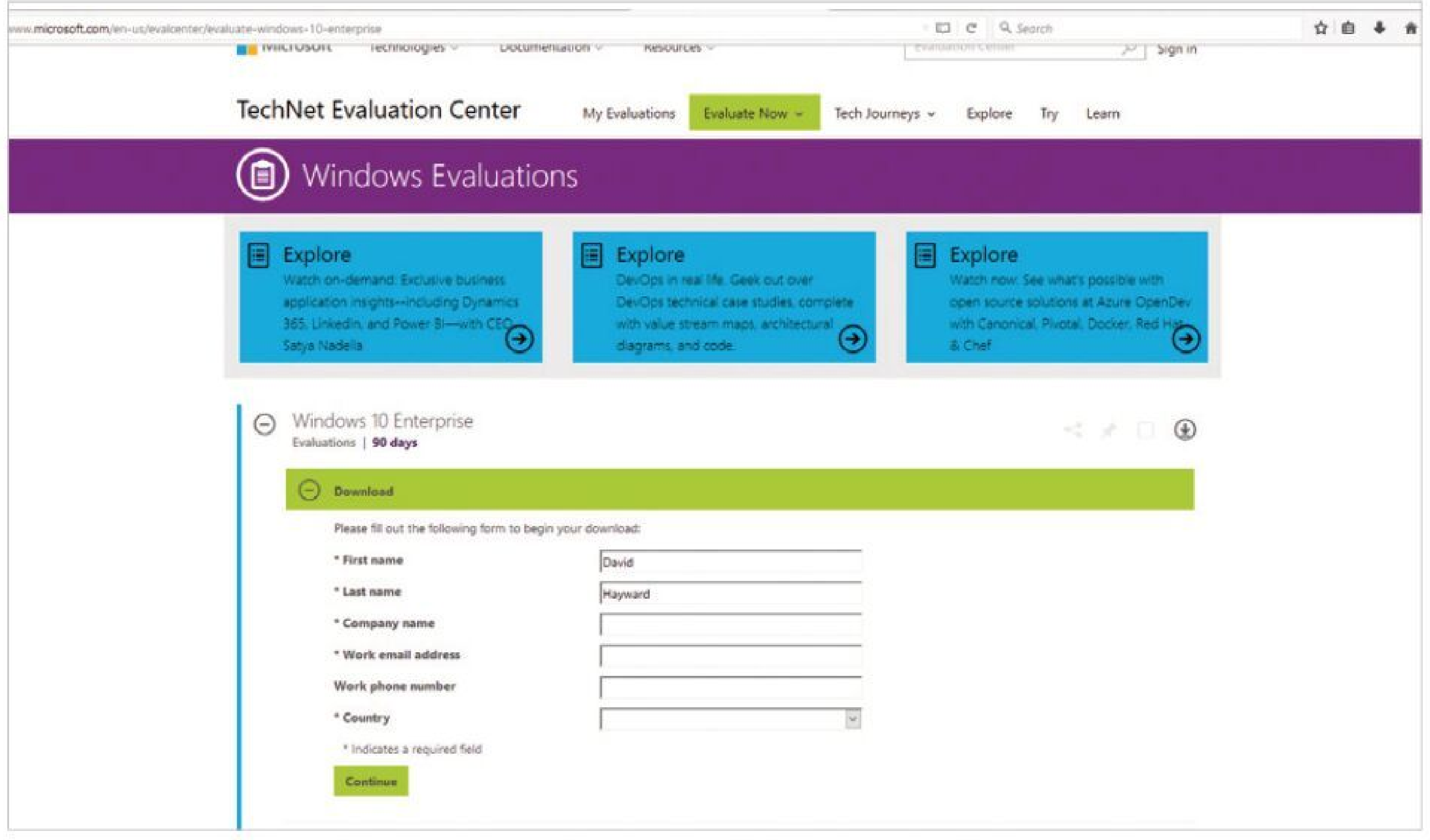
Installing Windows 10 in VirtualBox

Installing Windows 10 within a VM carries with it a clause: you need to make sure you have a valid license. However, if you're testing something then you can use the Windows 10 Enterprise Evaluation image, which will last for 90 days.

Window Installations

Naturally you might own a spare Windows 10 license to use for the VM but for this tutorial we're going for the 90 day Windows 10 Enterprise Evaluation model. To begin with, browse to https://microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise.

STEP 1 You need to register with Microsoft prior to being able to download the Windows 10 image; simply click the Register button and fill in the required fields. When done, click Continue and choose the ISO Enterprise option, then your language choice and 64-bit, followed by the Continue button once more to begin the download.



www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise

TechNet Evaluation Center

Windows Evaluations

Explore
Watch on-demand: Exclusive business application insights—including Dynamics 365, LinkedIn, and Power BI—with CEO Satya Nadella

Explore
DevOps in real life. Geek out over DevOps technical case studies, complete with value stream maps, architectural diagrams, and code.

Explore
Watch now. See what's possible with open source solutions at Azure OpenDev with Canonical, Pivotal, Docker, Red Hat & Chef

Windows 10 Enterprise
Evaluations | 90 days

Download

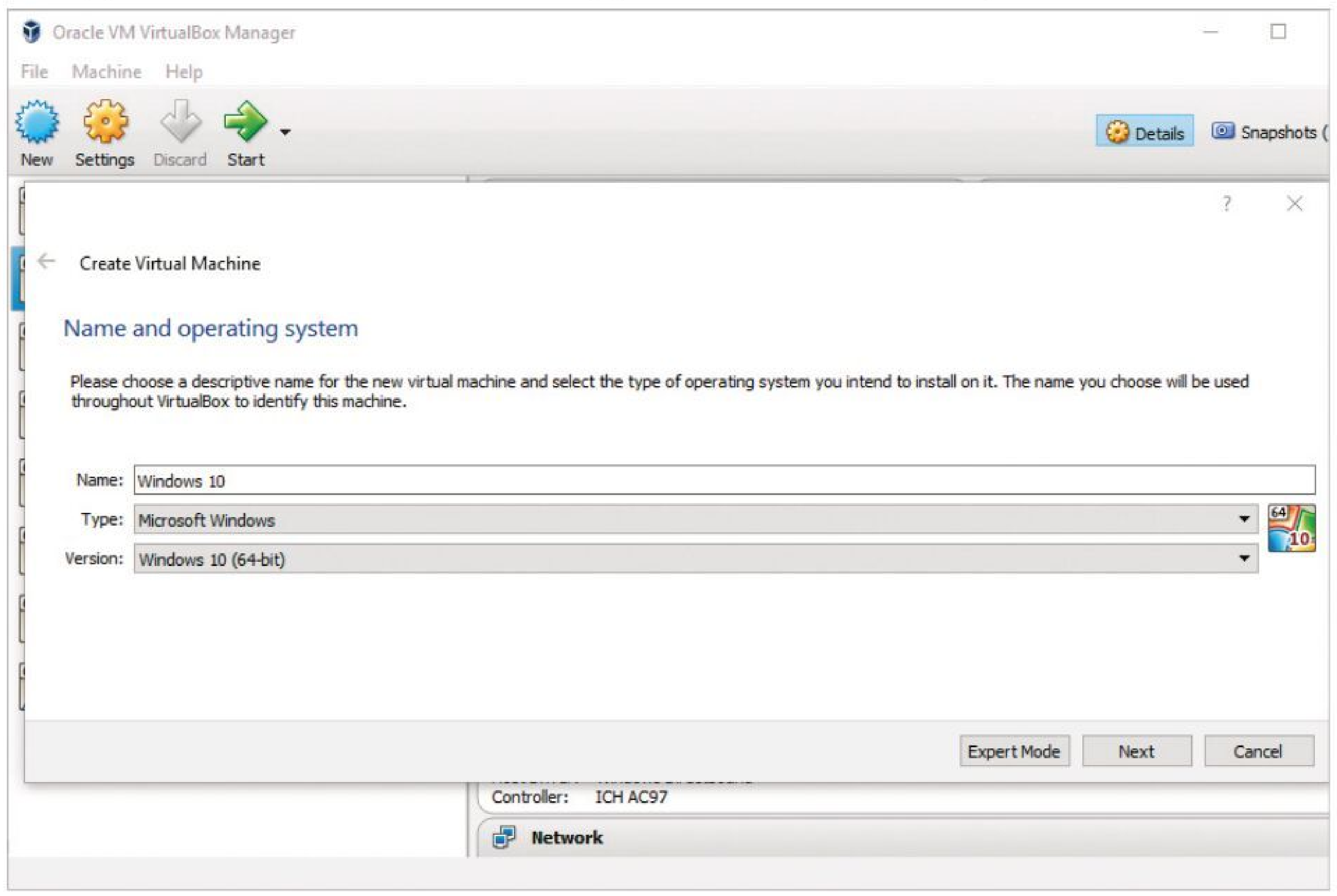
Please fill out the following form to begin your download:

* First name: David
* Last name: Hayward
* Company name:
* Work email address:
Work phone number:
* Country:

* Indicates a required field

Continue

STEP 2 The ISO you're downloading is around 4GB in size, so it may take some time, depending on the speed of your connection. Open VirtualBox and click on the New icon located in the top right of the main VirtualBox window. In the Name field enter Windows 10, this should automatically change the Type and Version fields accordingly. Click Next when ready.



Oracle VM VirtualBox Manager

Create Virtual Machine

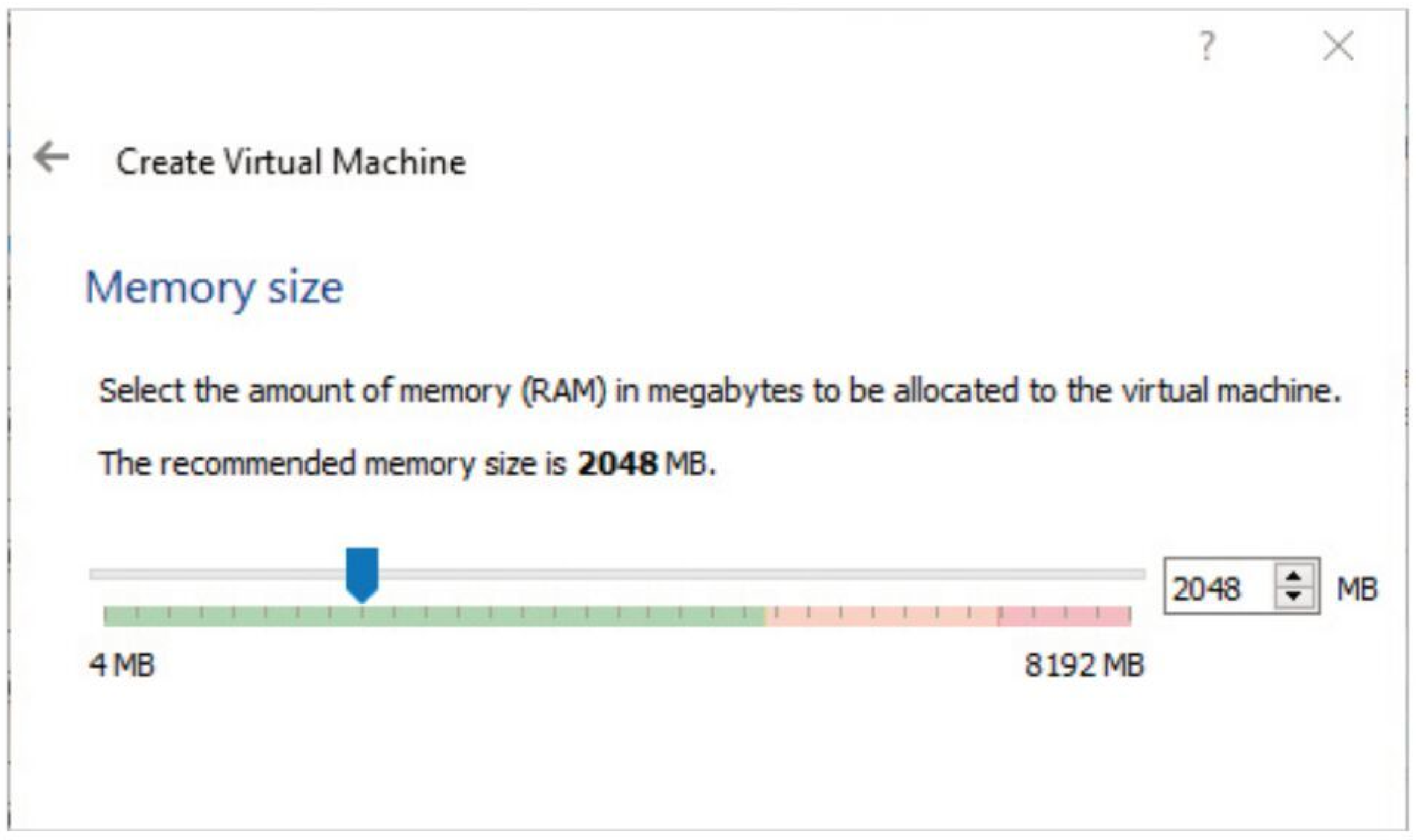
Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Windows 10
Type: Microsoft Windows
Version: Windows 10 (64-bit)

Controller: ICH AC97

STEP 3 You need to set an amount of memory from your host computer to use as virtual RAM for the VM. Naturally, you don't want to take too much as your computer will suffer due to low memory when the VM is running. Ideally, you need to allocate around 2GB of memory to the VM. Click Next when ready.



Create Virtual Machine

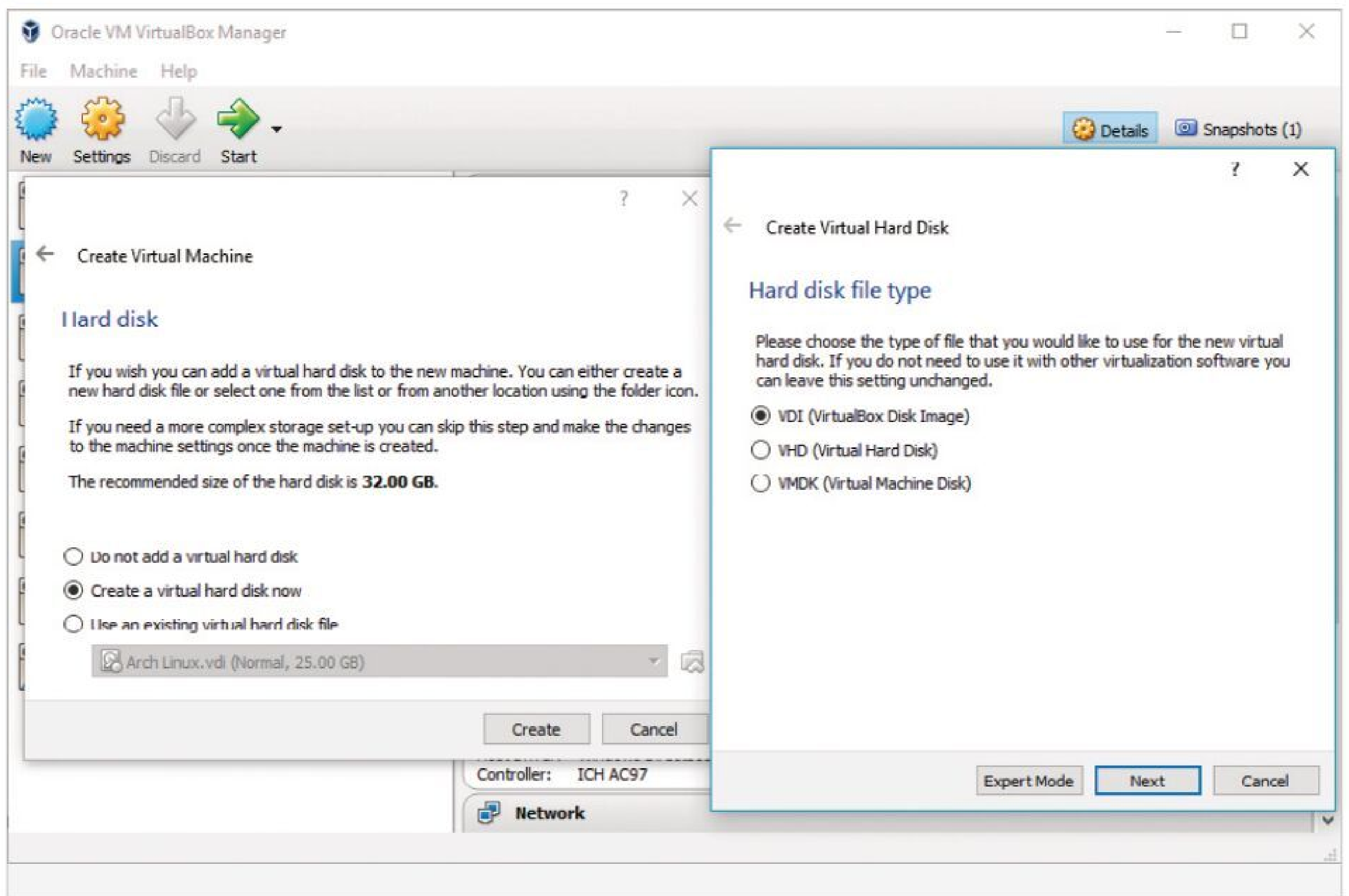
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **2048** MB.

2048 MB

STEP 4 The next section will enable you to create a virtual hard disk, in which the Windows 10 virtual machine can be installed. The default option: 'Create a virtual hard disk now' is recommended, then click the Create button to proceed. The pop-up box will detail the type of virtual hard disk; stick to VDI and click Next.



Oracle VM VirtualBox Manager

Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **32.00 GB**.

○ Do not add a virtual hard disk
● Create a virtual hard disk now
○ Use an existing virtual hard disk file

Arch Linux.vdi (Normal, 25.00 GB)

Create Virtual Hard Disk

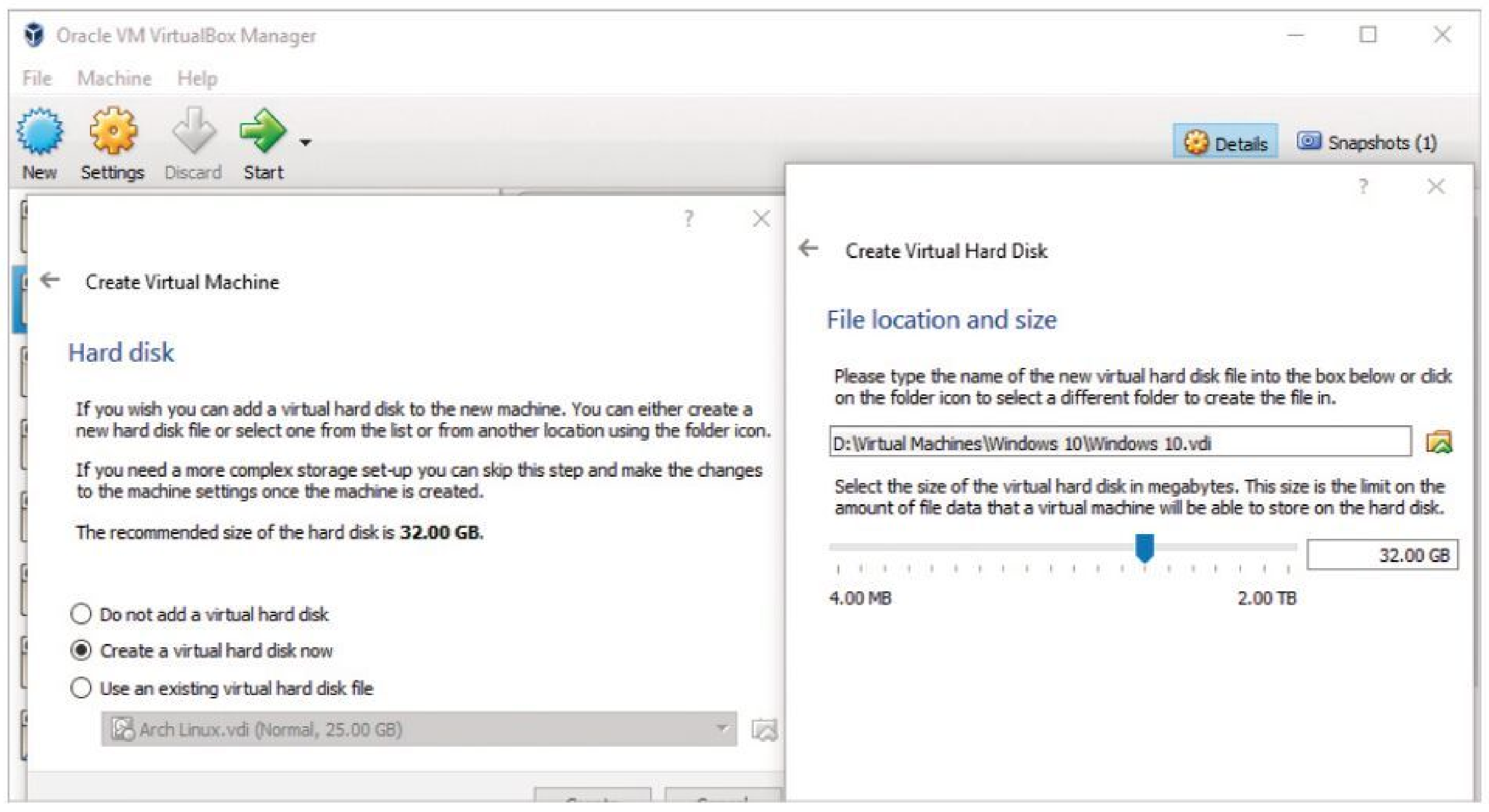
Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)
○ VHD (Virtual Hard Disk)
○ VMDK (Virtual Machine Disk)

Controller: ICH AC97

STEP 5 The default Dynamically Allocated option will suffice for this instance, so click Next. VirtualBox recommends that you allocate 32GB of physical hard drive space to creating the virtual hard disk. Make sure your hard drive has enough spare capacity and click the Create button.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots (1)

Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **32.00 GB**.

○ Do not add a virtual hard disk
● Create a virtual hard disk now
○ Use an existing virtual hard disk file
Arch Linux.vdi (Normal, 25.00 GB)

Create Virtual Hard Disk

File location and size

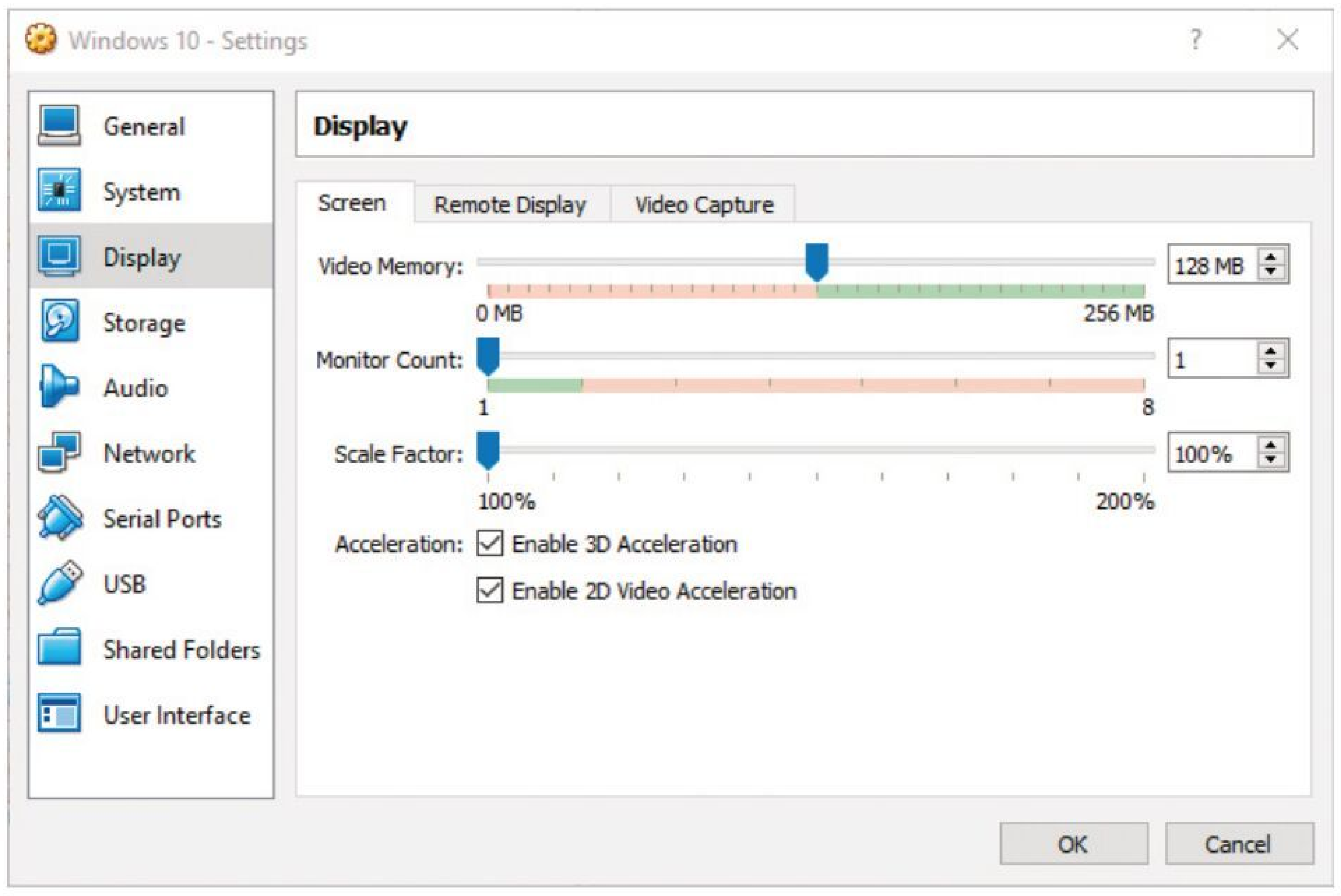
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

D:\Virtual Machines\Windows 10\Windows 10.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

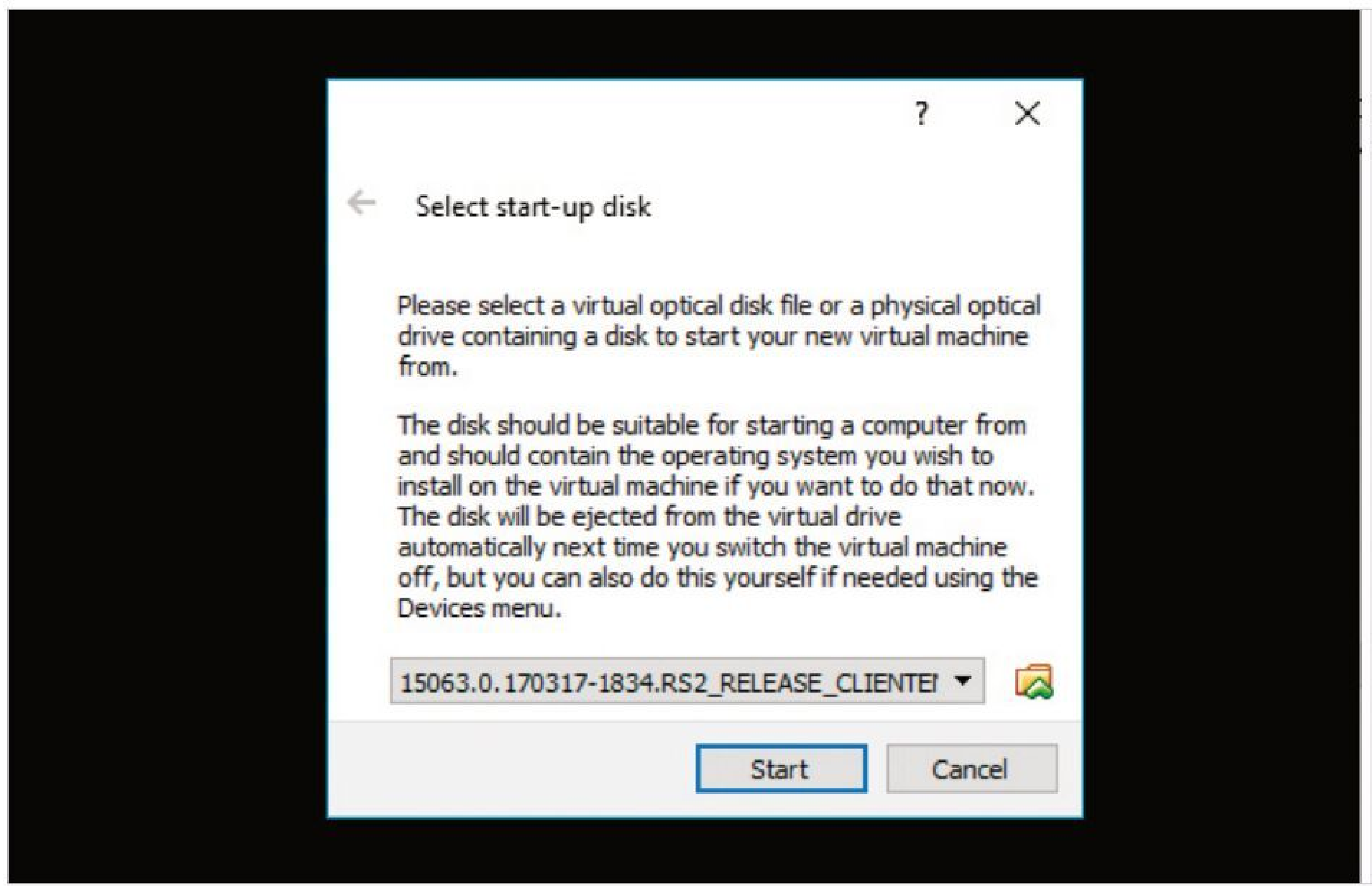
32.00 GB
4.00 MB
2.00 TB

STEP 6 The Windows 10 VM is now listed in the available VMs in VirtualBox. Before you begin to install it though, click on the Settings icon whilst the Windows 10 VM is highlighted. In the General tab, click Advanced and enable Bidirectional for Shared Clipboard and Drag 'n' Drop. In Display, enable 3D and 2D Video Acceleration. Click OK to finish.


Windows 10 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Display
Screen
Remote Display
Video Capture
0 MB
256 MB
1
8
100%
200%
OK
Cancel

Video Memory: 128 MB
Monitor Count: 1
Scale Factor: 100%
Acceleration: ☑ Enable 3D Acceleration
☑ Enable 2D Video Acceleration

STEP 7 With the Settings console window closed, and the VM highlighted, click on the Start button. This will open a new window, asking for the location of the Windows 10 ISO you downloaded from the Microsoft site in the first few steps. Use the folder icon to locate the ISO and click Open, then the Start button to commence the installation.

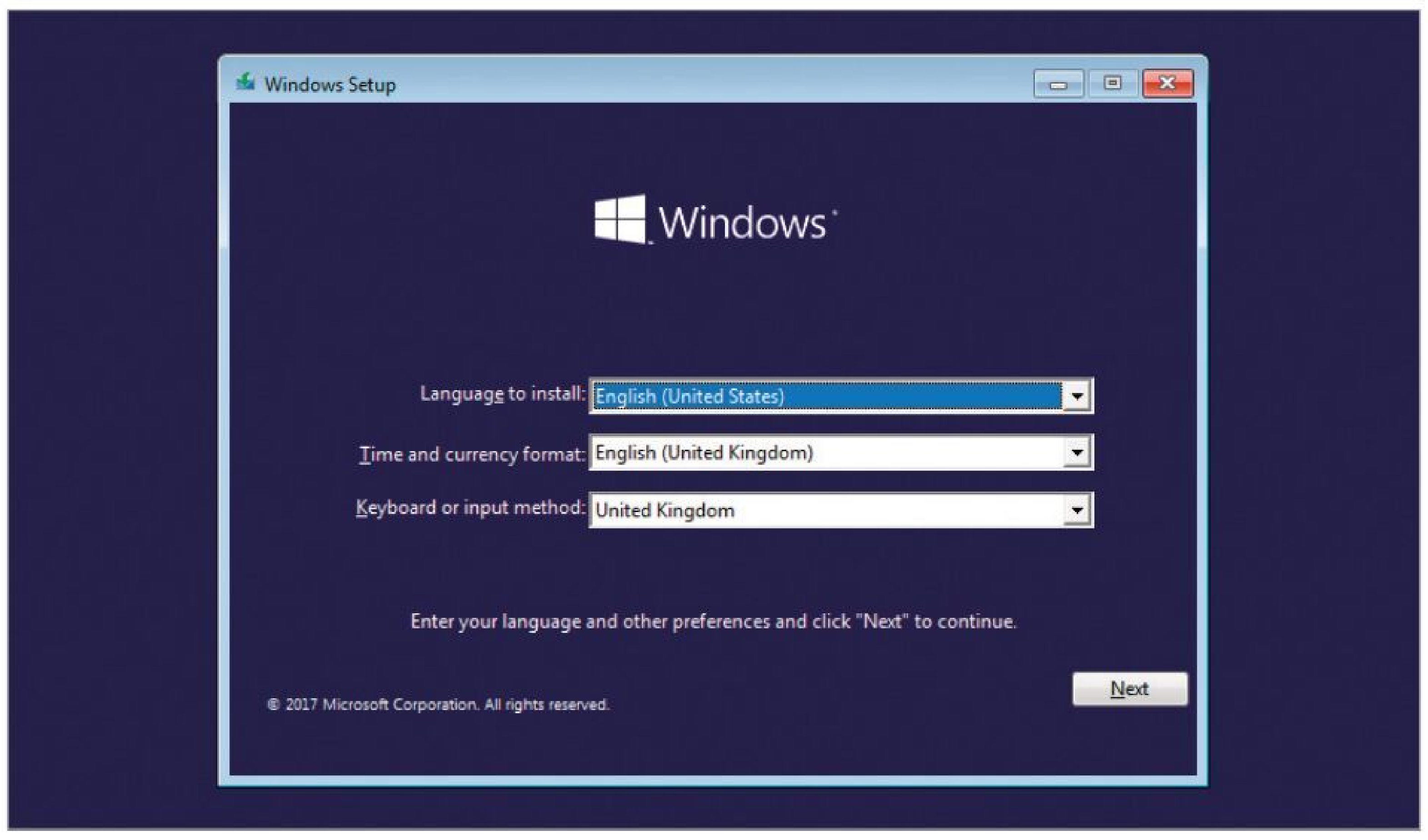

Select start-up disk

Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.

The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.

15063.0.170317-1834.RS2_RELEASE_CLIENTEI
Start
Cancel

STEP 8 The Windows ISO will now load, and begin the installation process. The first options you need to set are the language, time and keyboard. Set your preferences, although the default is English US to begin with, and click on the Next button when you're ready to continue.

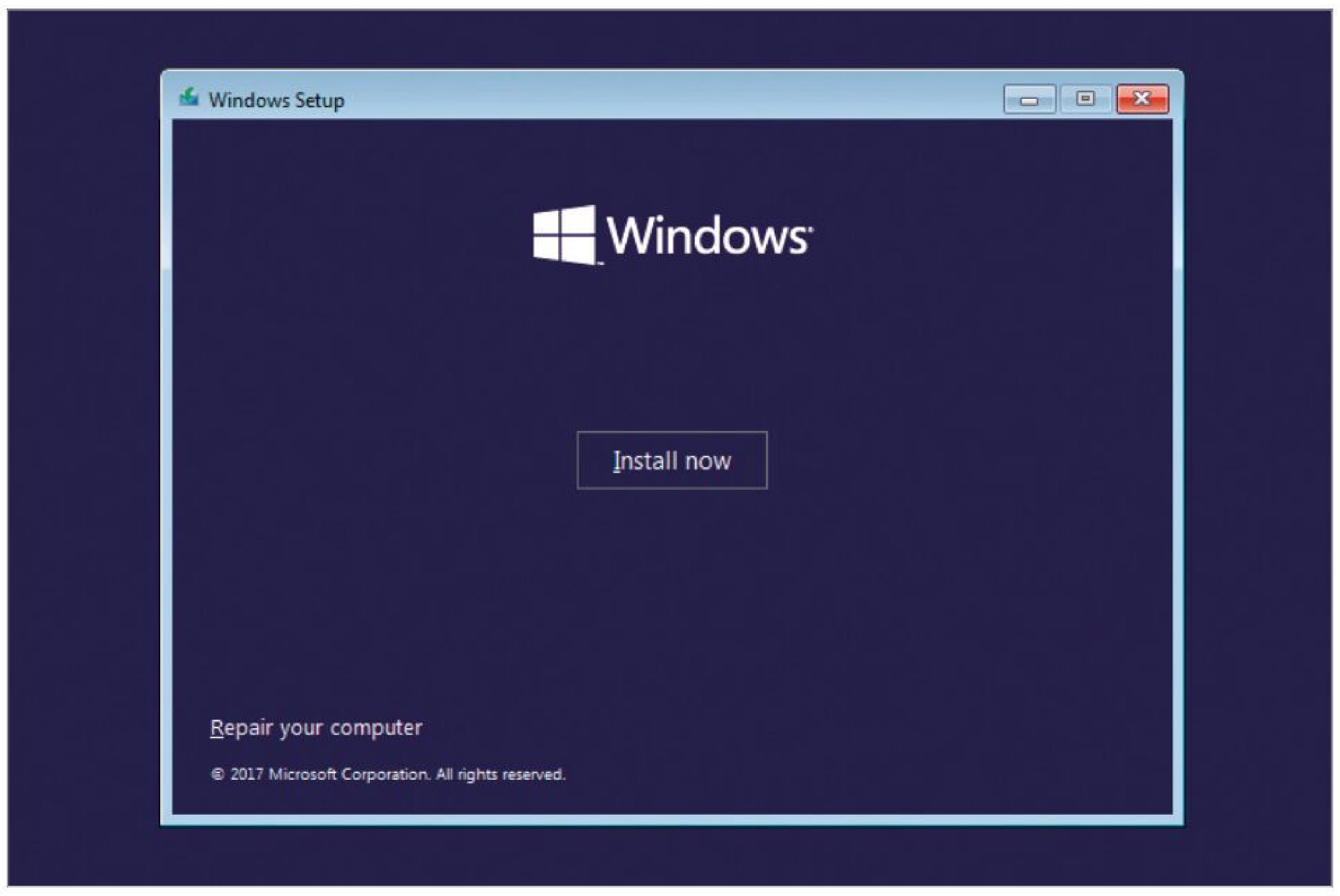

Windows Setup
Windows
Next

Language to install: English (United States)
Time and currency format: English (United Kingdom)
Keyboard or input method: United Kingdom

Enter your language and other preferences and click "Next" to continue.

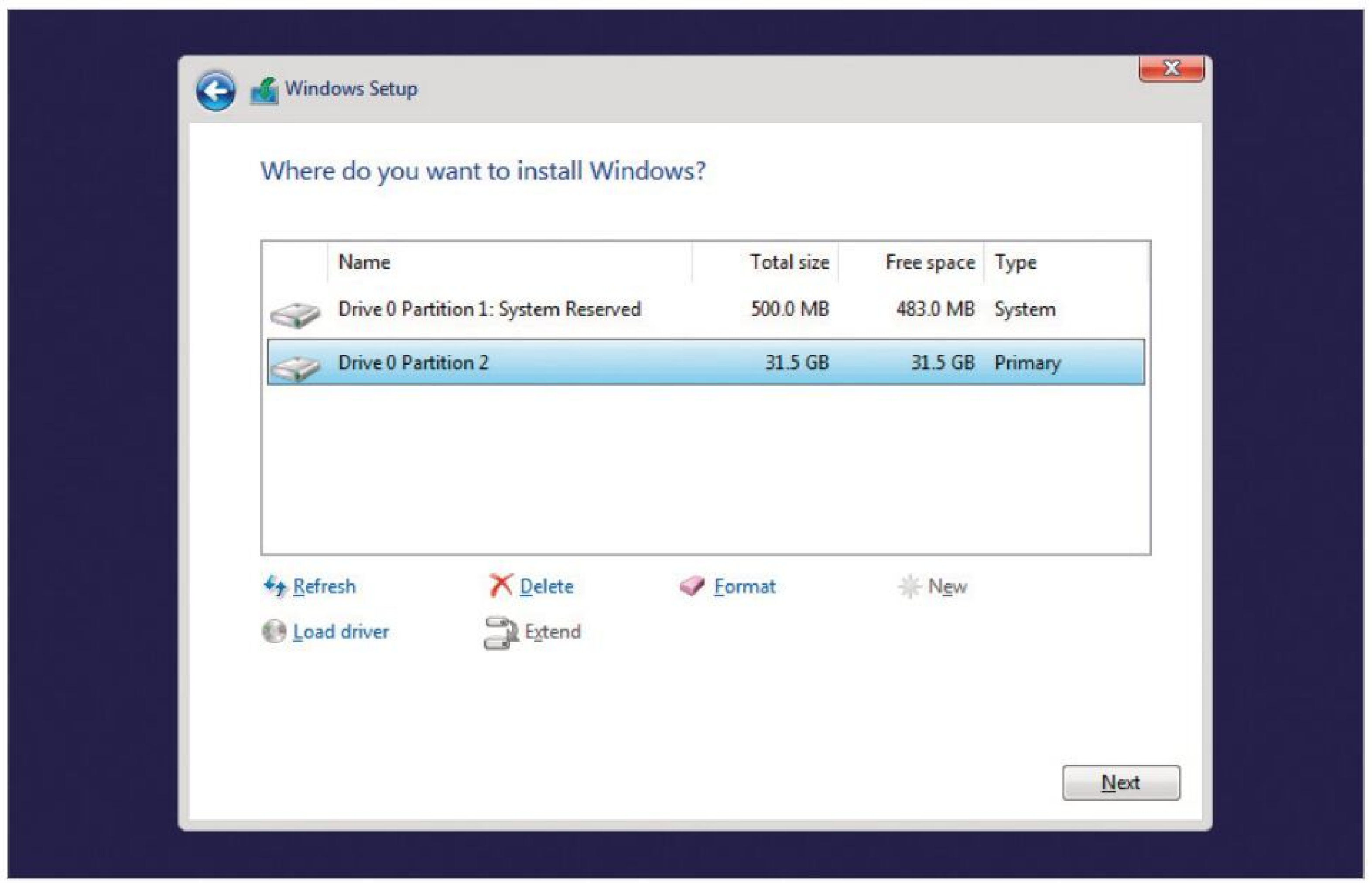
© 2017 Microsoft Corporation. All rights reserved.

STEP 9 You now have an Install Now option available. Click it to begin the installation, then tick the license agreement box followed by Next. There are two possible options to install Windows 10, Upgrade and Custom. Since this is a blank hard drive, the Custom option is the only viable mode. Click it to continue.


Windows Setup
Windows
Install now
Repair your computer

© 2017 Microsoft Corporation. All rights reserved.

STEP 10 The drive available will be the 32GB virtual hard disk you created. Click on the New button, then Apply to create a new valid drive that Windows 10 can be installed on. You'll be asked what additional partitions will be created, click OK to accept. Choose the largest partition size and click Next to install Windows 10.


Windows Setup
Refresh
Delete
Format
New
Load driver
Extend
Next

Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Partition 1: System Reserved	500.0 MB	483.0 MB	System
Drive 0 Partition 2	31.5 GB	31.5 GB	Primary

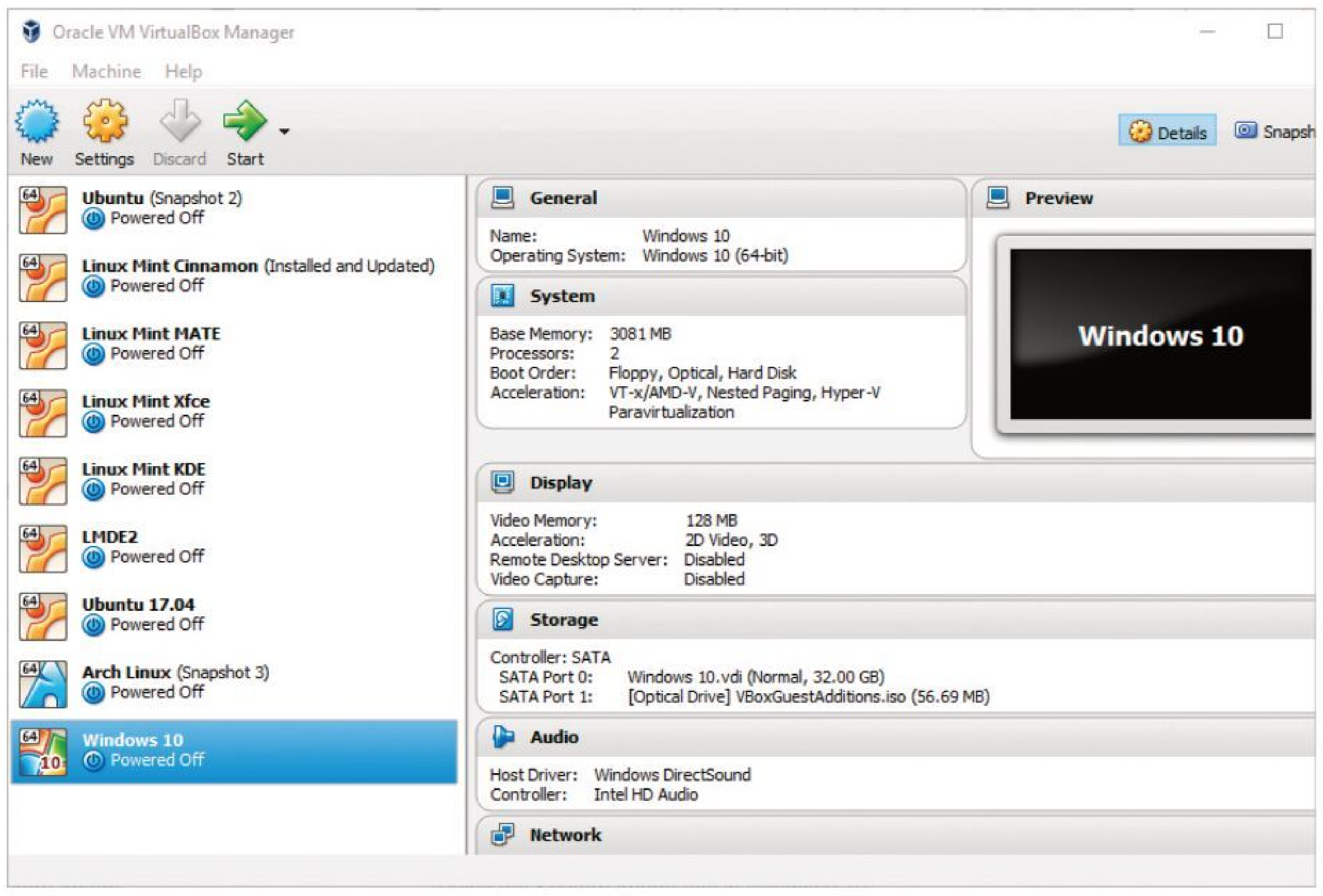
Creating VirtualBox Snapshots of Windows 10

One day the testing process of a Windows 10 VM will inevitably leave the system in a broken or malware riddled state. You can wipe it and start again but a far better solution is to create snapshots, so you can easily revert to a previous build.

Take a Snapshot

Setting up Windows 10, installing the drivers, updates and programs takes a fair amount of time. If you take a VirtualBox snapshot, you can return to where you left off in an instant.

STEP 1 To begin with open VirtualBox. If it's already open, shutdown the Windows 10 VirtualBox image you created. It's not necessary but it's often easier, to ensure the VM is closed prior to creating a snapshot.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapsh
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 Powered Off
General
Preview
Windows 10
System
Display
Storage
Audio
Network

Name: Windows 10
Operating System: Windows 10 (64-bit)

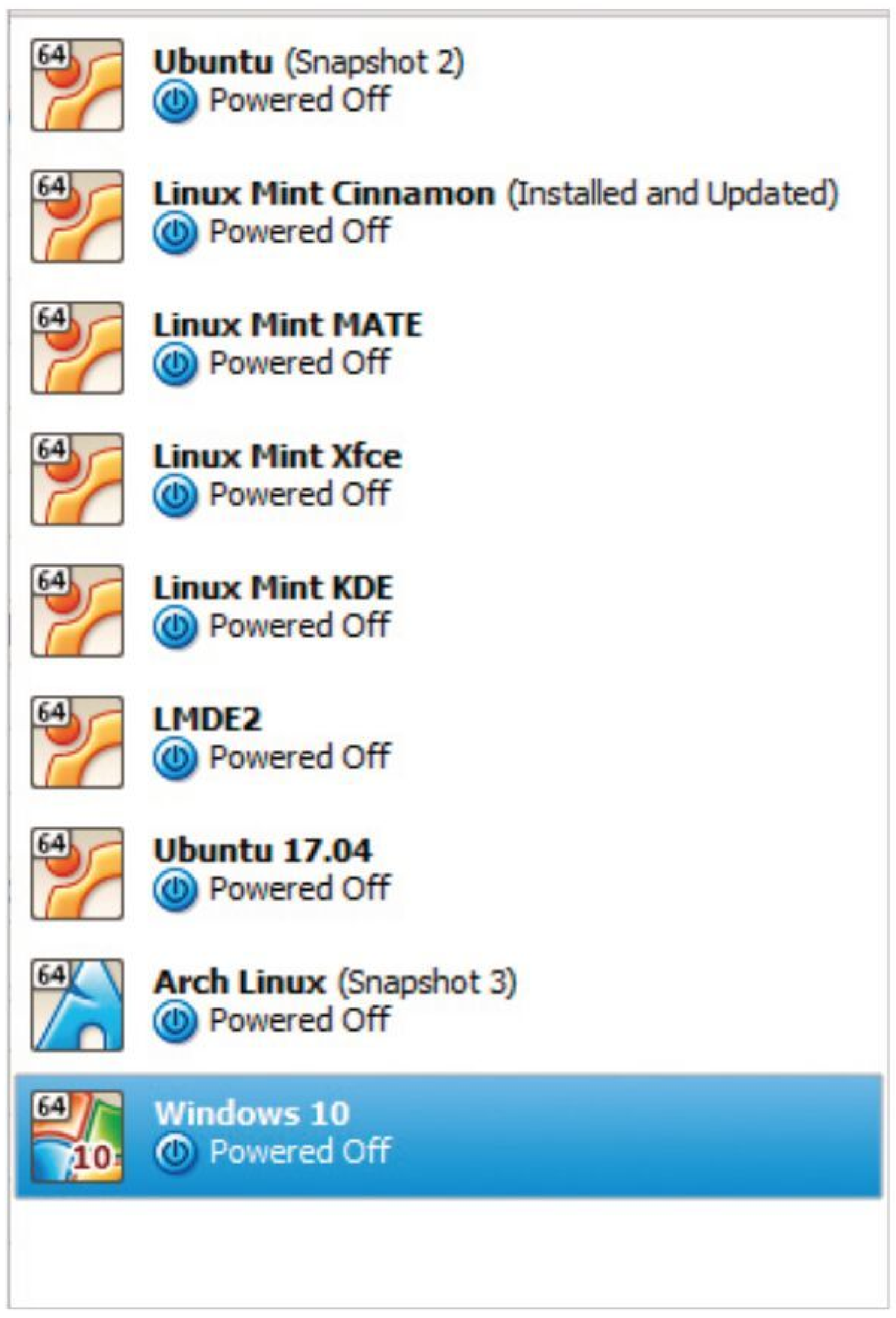
Base Memory: 3081 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Video Memory: 128 MB
Acceleration: 2D Video, 3D
Remote Desktop Server: Disabled
Video Capture: Disabled

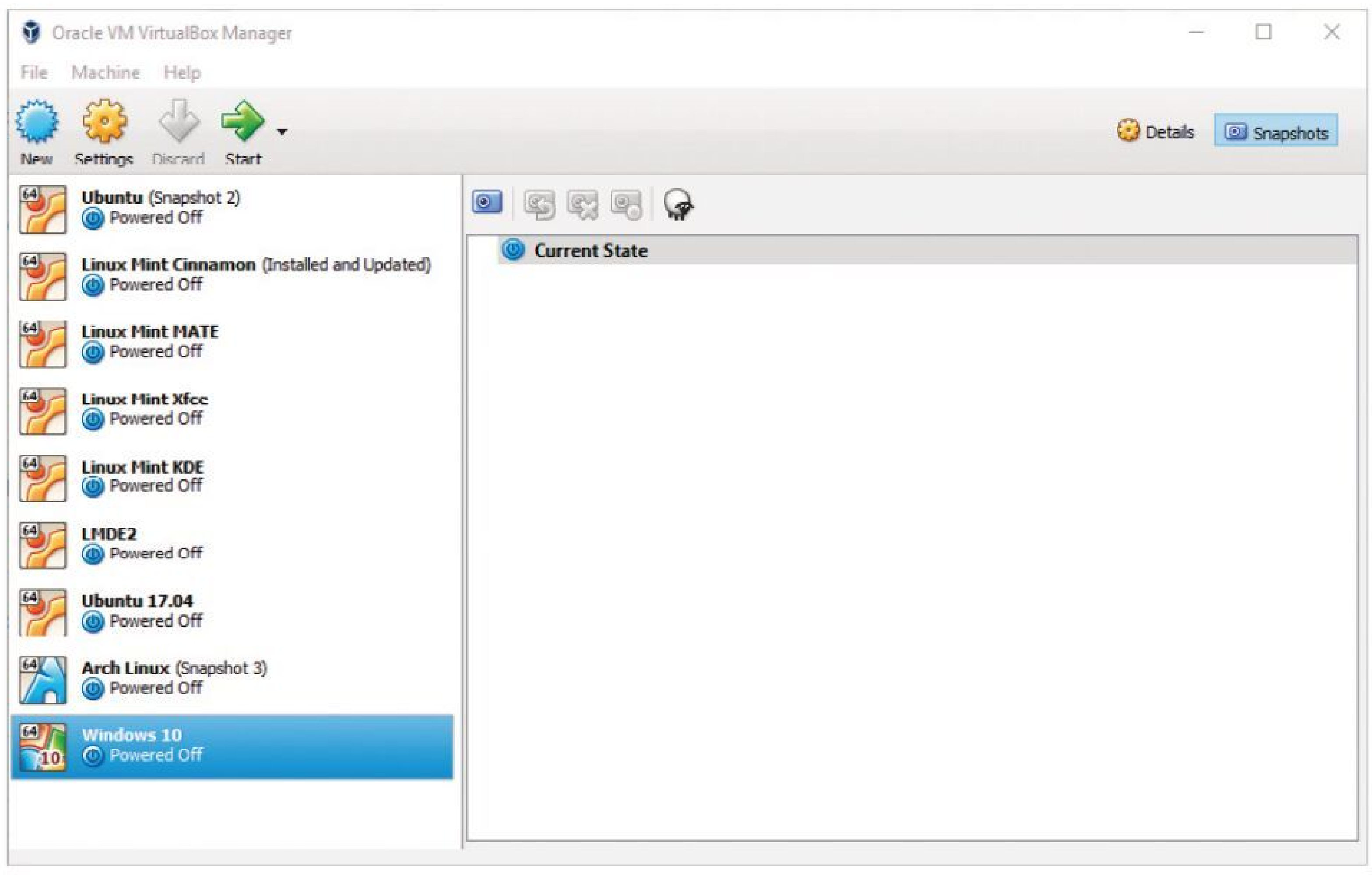
Controller: SATA
SATA Port 0: Windows 10.vdi (Normal, 32.00 GB)
SATA Port 1: [Optical Drive] VBoxGuestAdditions.iso (56.69 MB)

Host Driver: Windows DirectSound
Controller: Intel HD Audio

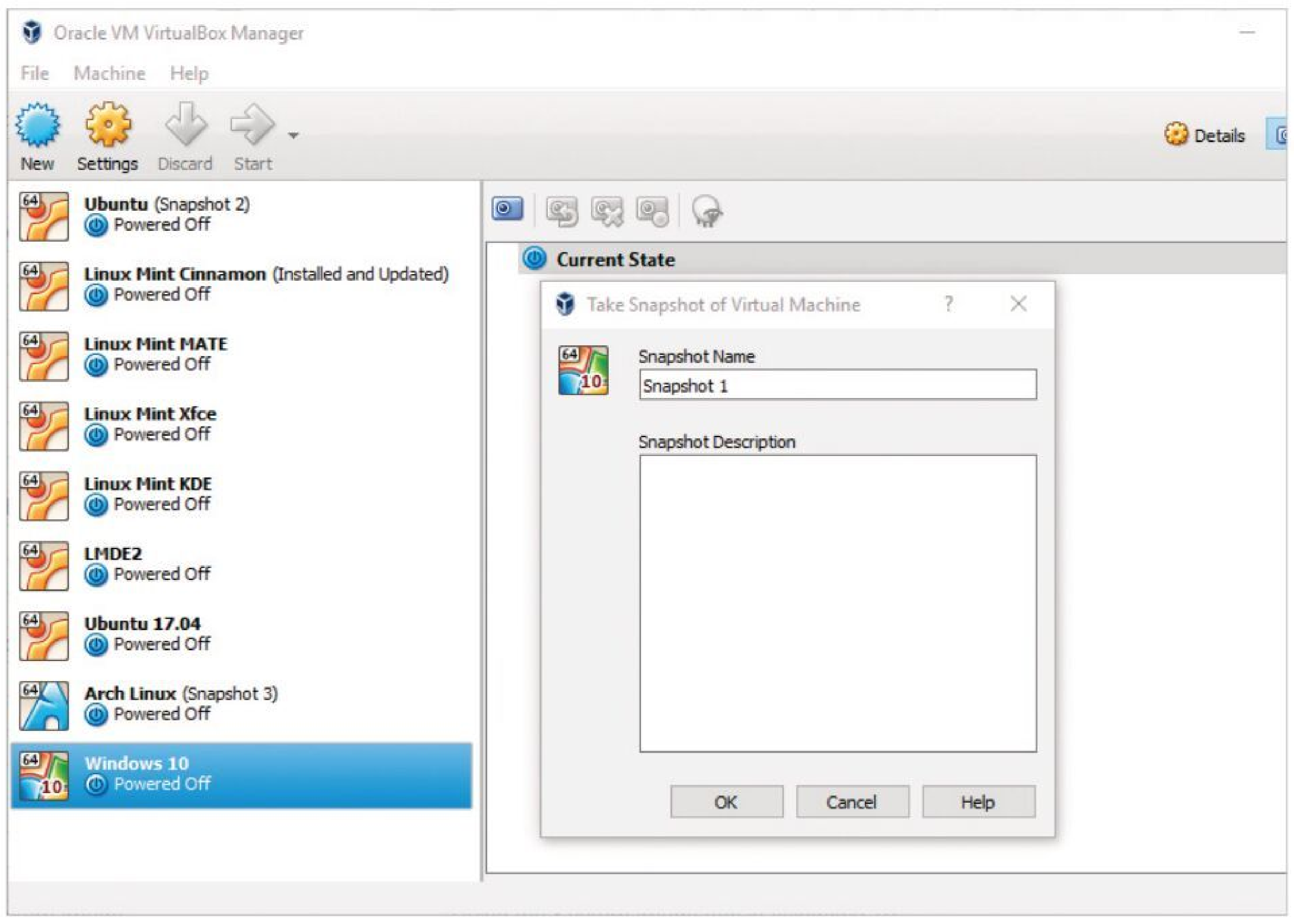
STEP 2 A Snapshot in VirtualBox is simply an image of what the virtual machine 'looked' like at the time the Snapshot was taken. You can make multiple Snapshots and revert to any whenever you wish. Snapshots taken are labelled next to the name of the VM.


Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 Powered Off

STEP 3 You can see that the state of all the virtual systems is currently Powered Off. To create a Snapshot of the Windows 10 VM, click to highlight the system's entry in VirtualBox, then click on the Snapshots button (it's a camera icon), located to the far-right of the VirtualBox console.

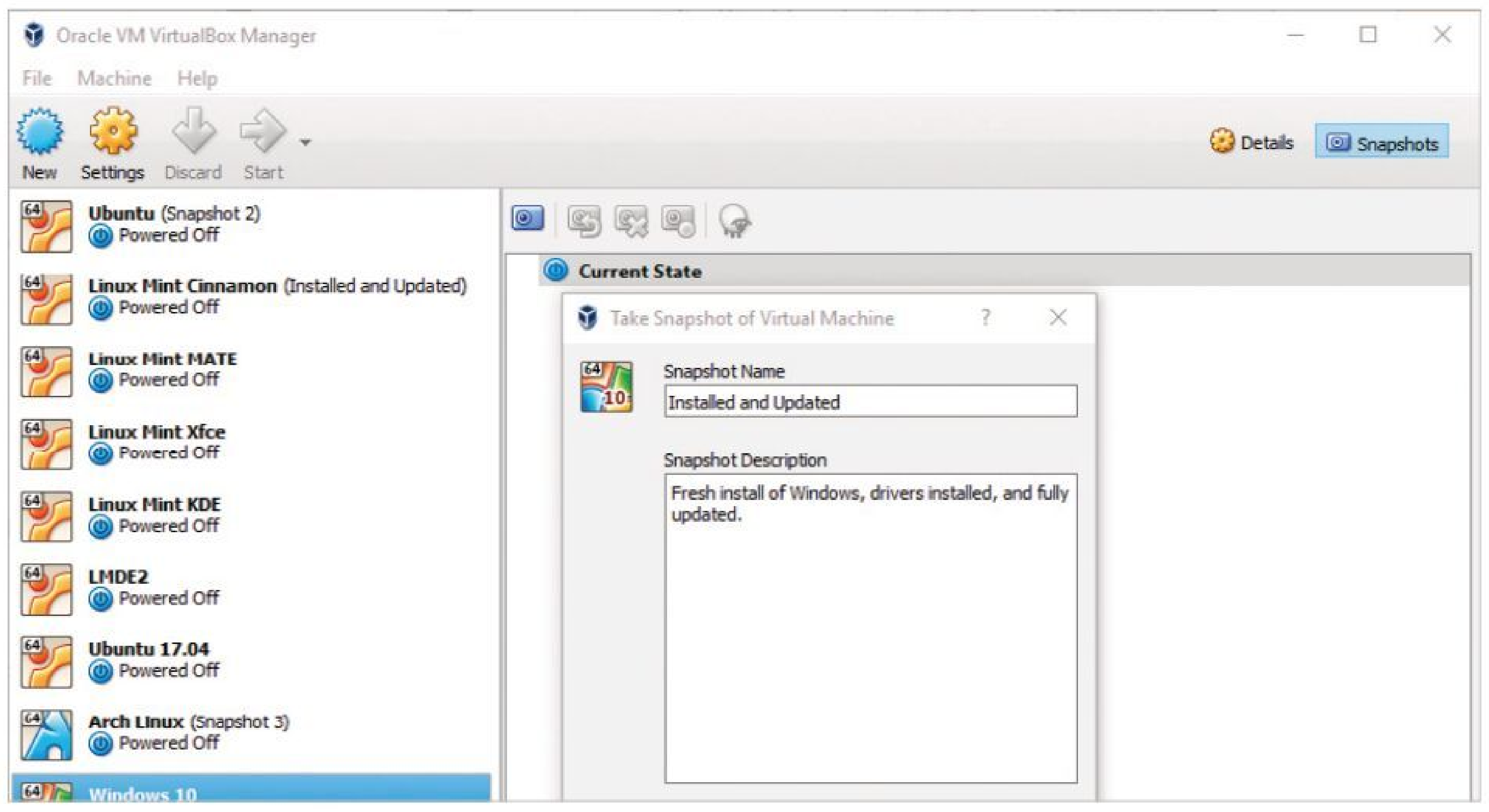

Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 Powered Off
Current State

STEP 4 At present there aren't any Snapshots of Windows 10 available. To create one, click the camera icon just above the words Current State, the icon at the opposite end of the sheep icon. This will launch the Take Snapshot of Virtual Machine console window.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 Powered Off
Current State
Take Snapshot of Virtual Machine
Snapshot Description
OK
Cancel
Help

Snapshot Name: Snapshot 1

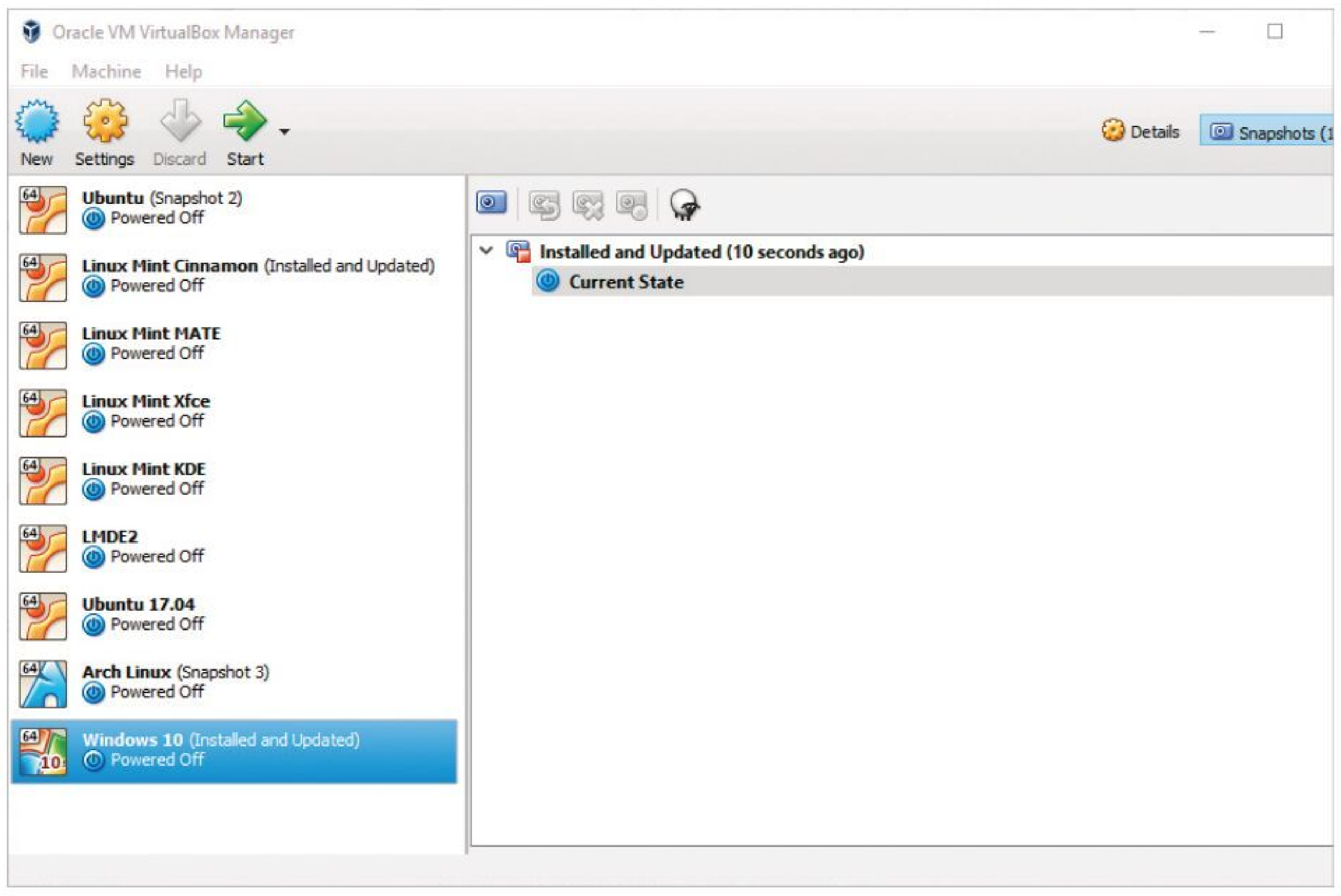
STEP 5 If you want you can name the Snapshot: Installed and Updated for example, along with a description to help identify it easier from the other Snapshots you may eventually end up making. It's not hugely important but if someone else wants to load up Windows 10, they know which Snapshot to go for. When you're done, click the OK button.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10
Current State
Take Snapshot of Virtual Machine

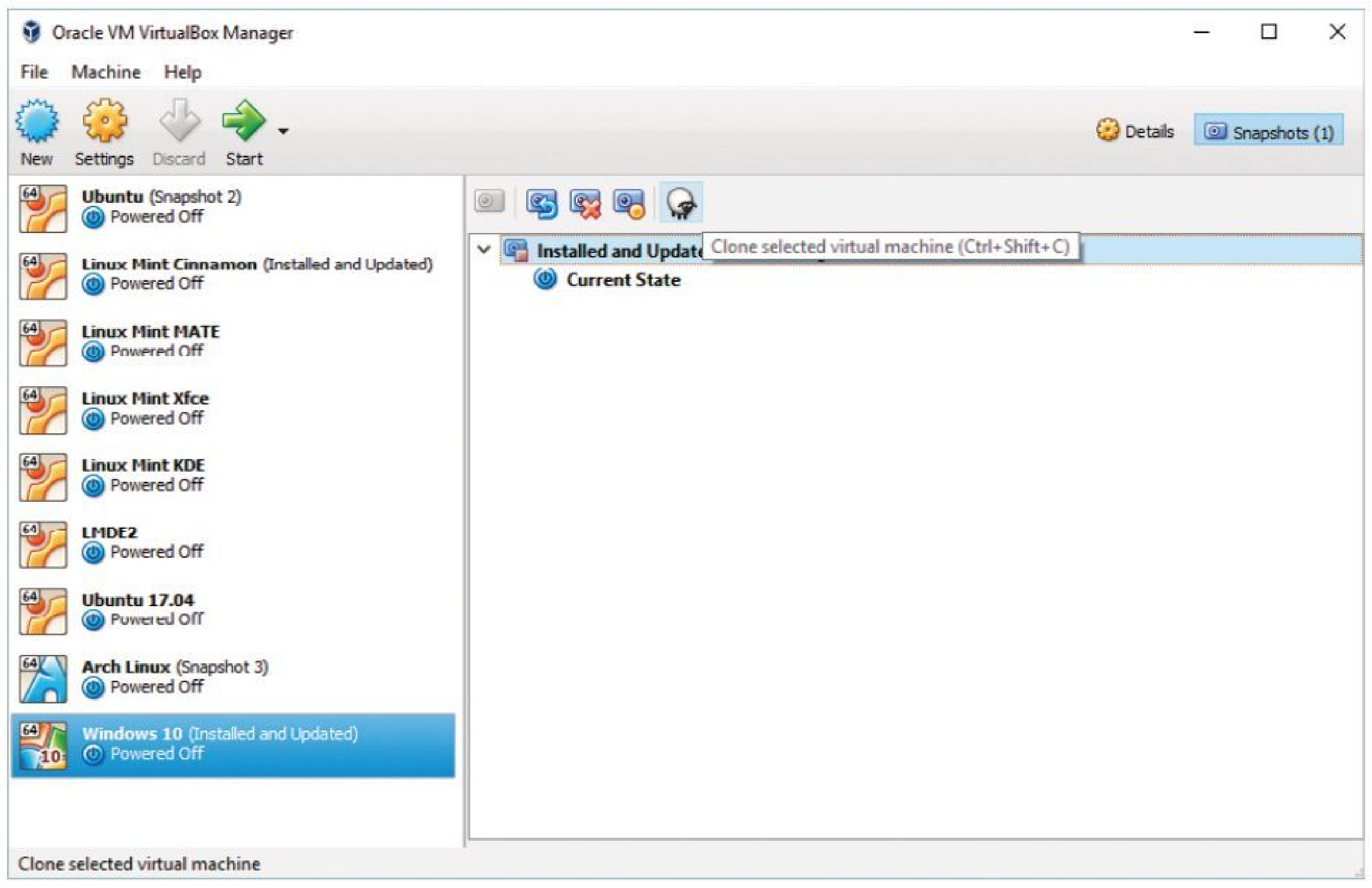
Snapshot Name: Installed and Updated

Snapshot Description: Fresh install of Windows, drivers installed, and fully updated.

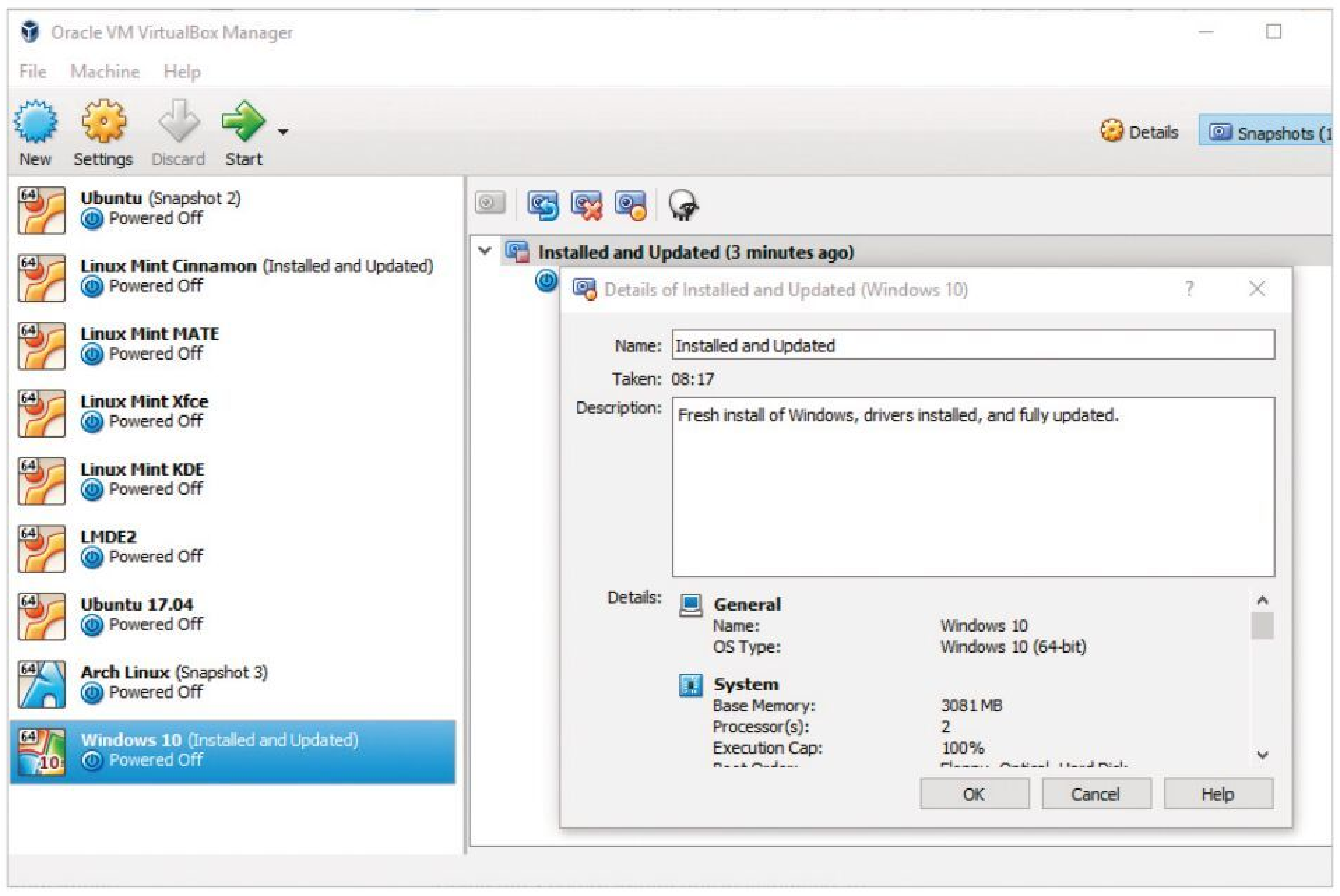
STEP 6 The process happens almost instantly and you're left with an entry in the Snapshots section detailing the named Snapshot, how long ago it was taken and a Current State entry. The Current State is literally its state when you boot it up. With it highlighted, you can take more Snapshots by using the camera icon again.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 (Installed and Updated) Powered Off
Installed and Updated (10 seconds ago)
Current State

STEP 7 If you click the named Snapshot, you get more options available in the toolbar just above. Here you can Restore a selected Snapshot, if you have multiple entries. You can Delete a Snapshot and view detailed information regarding one; and with the sheep, you can Clone the current Snapshot as a new virtual machine.

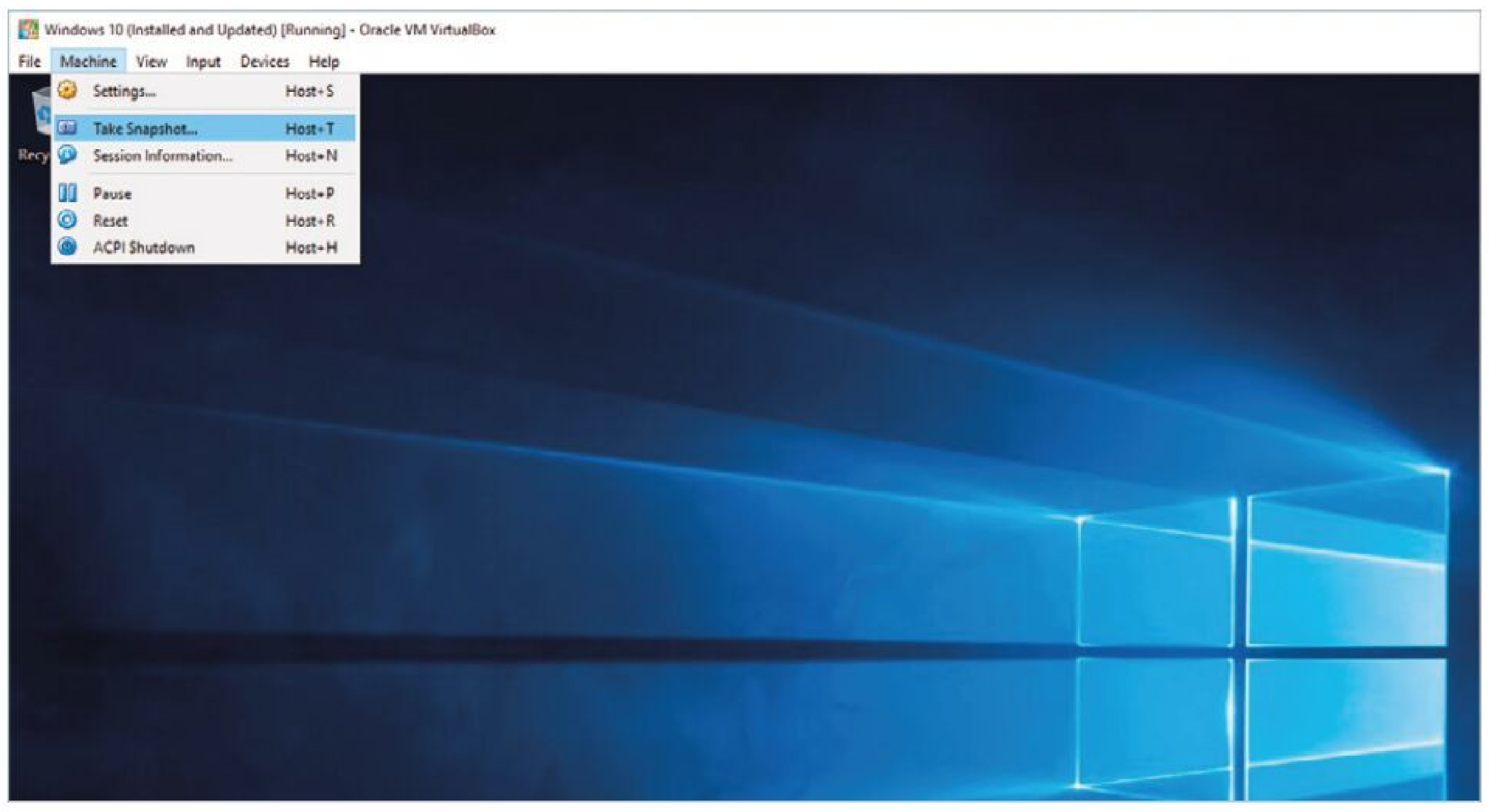

Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots (1)
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 (Installed and Updated) Powered Off
Installed and Update
Clone selected virtual machine (Ctrl+Shift+C)
Current State
Clone selected virtual machine

STEP 8 If you click the Details of the named virtual machine icon, the one next to the sheep, represented with an orange circle, you can view the VirtualBox settings of that particular Snapshot. This way you can assess any issues that may arise with other virtual machines; here you can see which settings worked and which didn't.

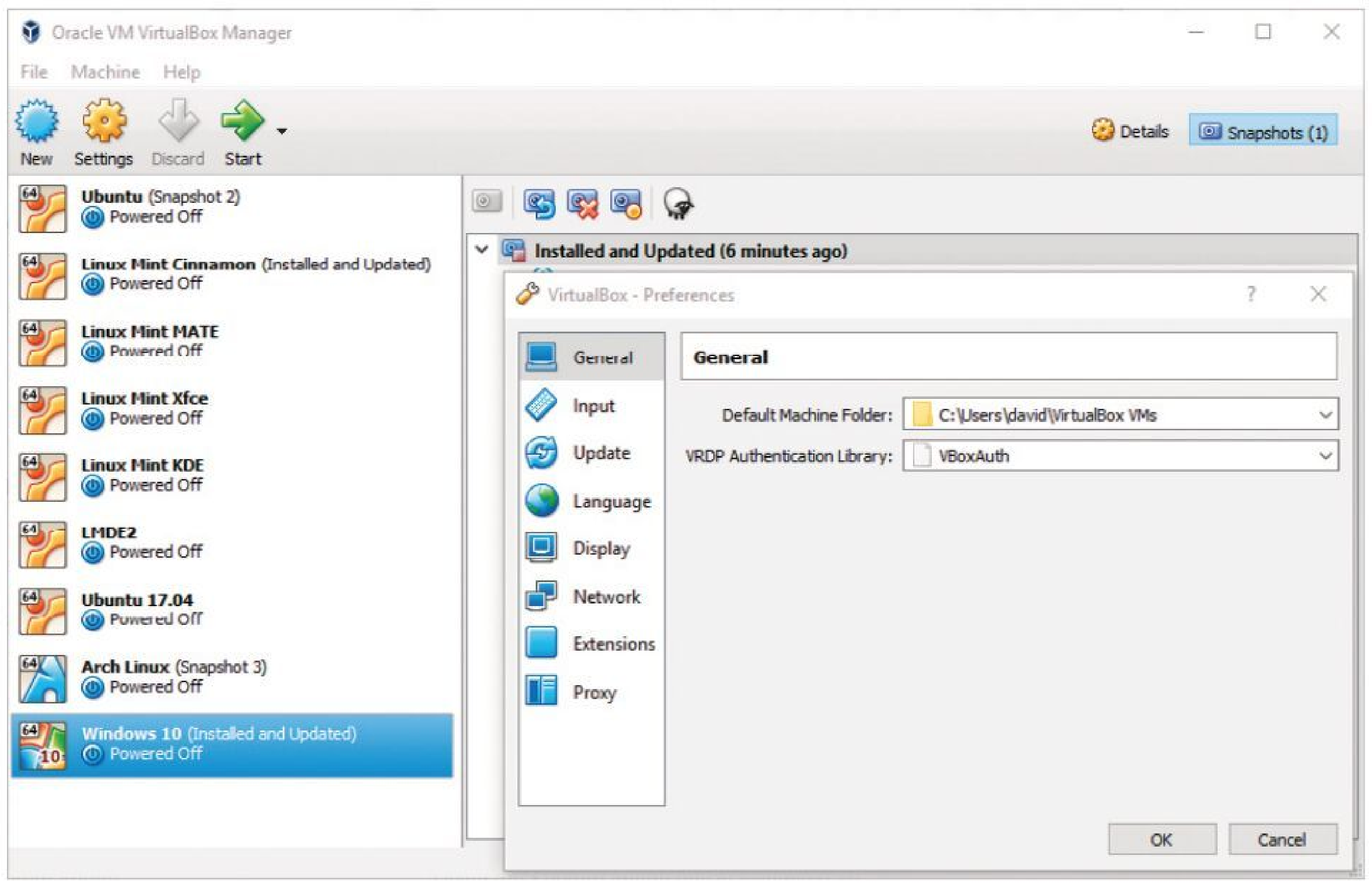

Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 (Installed and Updated) Powered Off
Installed and Updated (3 minutes ago)
Details of Installed and Updated (Windows 10)
OK Cancel Help

Name: Installed and Updated
Taken: 08:17
Description: Fresh install of Windows, drivers installed, and fully updated.
Details:
General
Name: Windows 10
OS Type: Windows 10 (64-bit)
System
Base Memory: 3081 MB
Processor(s): 2
Execution Cap: 100%

STEP 9 You shutdown the guest system, as mentioned in Step 1, but VirtualBox guest doesn't need to be shutdown in order for a Snapshot to be taken. For example, prior to installing an experimental program, click the Machine entry in the VirtualBox top menu bar and choose Take Snapshot. The process works the same way as in Steps 4 onward.


Windows 10 (Installed and Updated) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Settings... Host+S
Take Snapshot... Host+T
Session Information... Host+N
Pause Host+P
Reset Host+R
ACPI Shutdown Host+H

STEP 10 Each Snapshot taken can easily be reverted to, cloned, deleted and so on. However, Snapshots are stored by default in the Users/username/VirtualBox VMs folder in Windows. If you've only a limited amount of space on your C:\ drive, you may want to set the path to a bigger hard drive in the File > Preferences option in VirtualBox.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots (1)
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 (Installed and Updated) Powered Off
Installed and Updated (6 minutes ago)
VirtualBox - Preferences
General
Input
Update
Language
Display
Network
Extensions
Proxy
OK Cancel

General
Default Machine Folder: C:\Users\david\VirtualBox VMs
VRDP Authentication Library: VBoxAuth

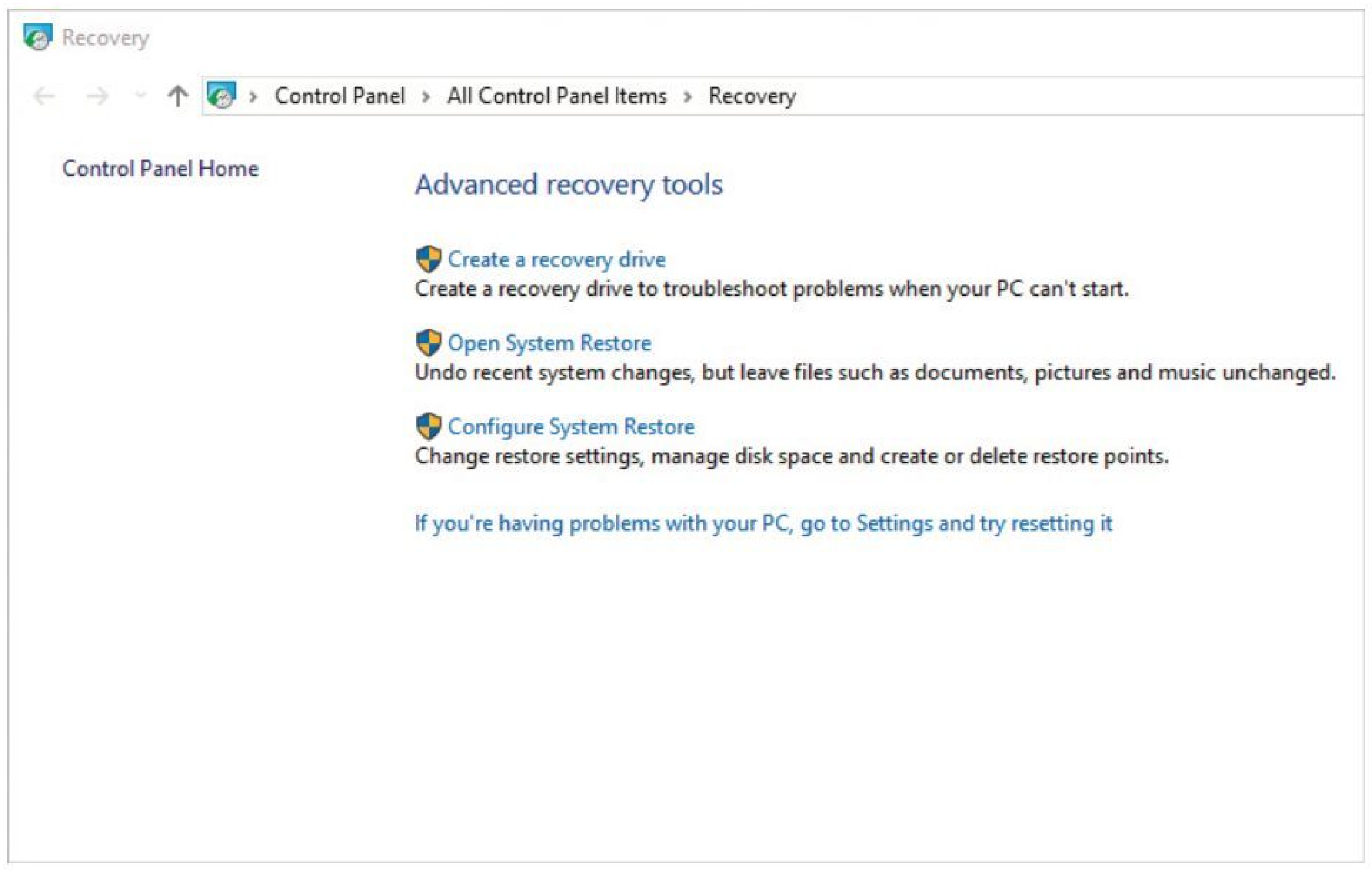
Create a Windows 10 Recovery Drive

Since Windows 95, Microsoft has offered users the ability to create a recovery drive, which is used to help troubleshoot a Windows PC that is failing to boot, by presenting various options. If you haven't done so yet, you ideally should have created a Windows 10 recovery drive.

Time to Recover

You need an 8GB USB drive minimum, in order to successfully create a recovery drive. It wipes the contents off the drive and you won't be able to use it for anything else, so make sure it's labelled and stored in a safe place.

STEP 1 Insert the USB drive into your PC and close the Explorer window that opens upon insertion. Click the Windows Start button and type recovery, then click on the Recovery Control Panel. In here you can see several options available; you want the first, Create a recovery drive.



Advanced recovery tools

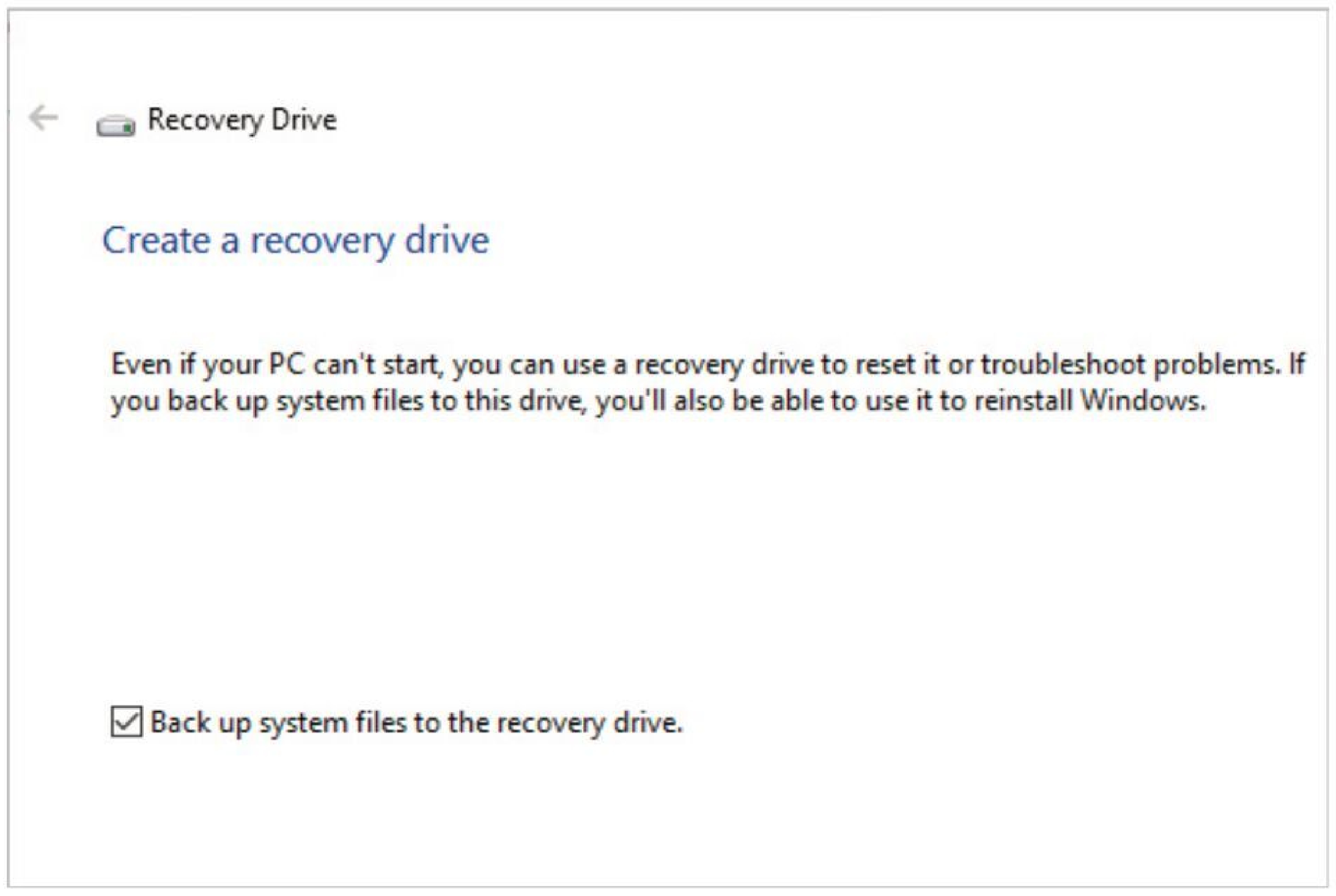
Create a recovery drive
Create a recovery drive to troubleshoot problems when your PC can't start.

Open System Restore
Undo recent system changes, but leave files such as documents, pictures and music unchanged.

Configure System Restore
Change restore settings, manage disk space and create or delete restore points.

If you're having problems with your PC, go to Settings and try resetting it

STEP 2 Click the Create a recovery drive link and accept the UAC authentication message that pops up. First, there's the option to backup any important system files to the recovery drive, alongside the usual recovery options. This is a good idea as it can replace these vital files in the event of a boot failure. Click Next to continue.

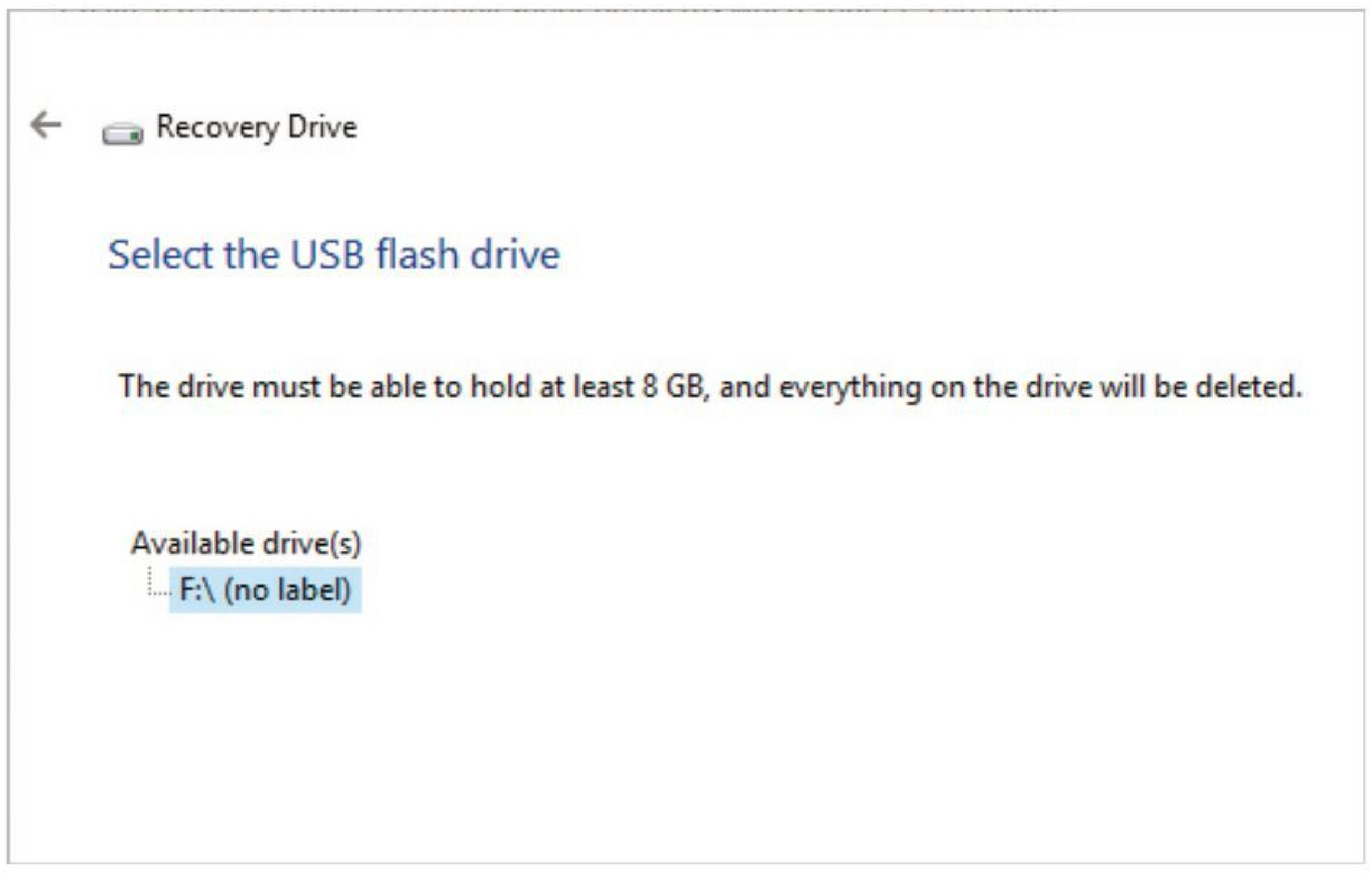


Create a recovery drive

Even if your PC can't start, you can use a recovery drive to reset it or troubleshoot problems. If you back up system files to this drive, you'll also be able to use it to reinstall Windows.

☑ Back up system files to the recovery drive.

STEP 3 There's a short wait as Windows analyses the available locations where it can install and create the recovery drive. Eventually, providing you inserted the 8GB plus USB stick prior to starting the process, you're asked to select the destination from those Windows has discovered.

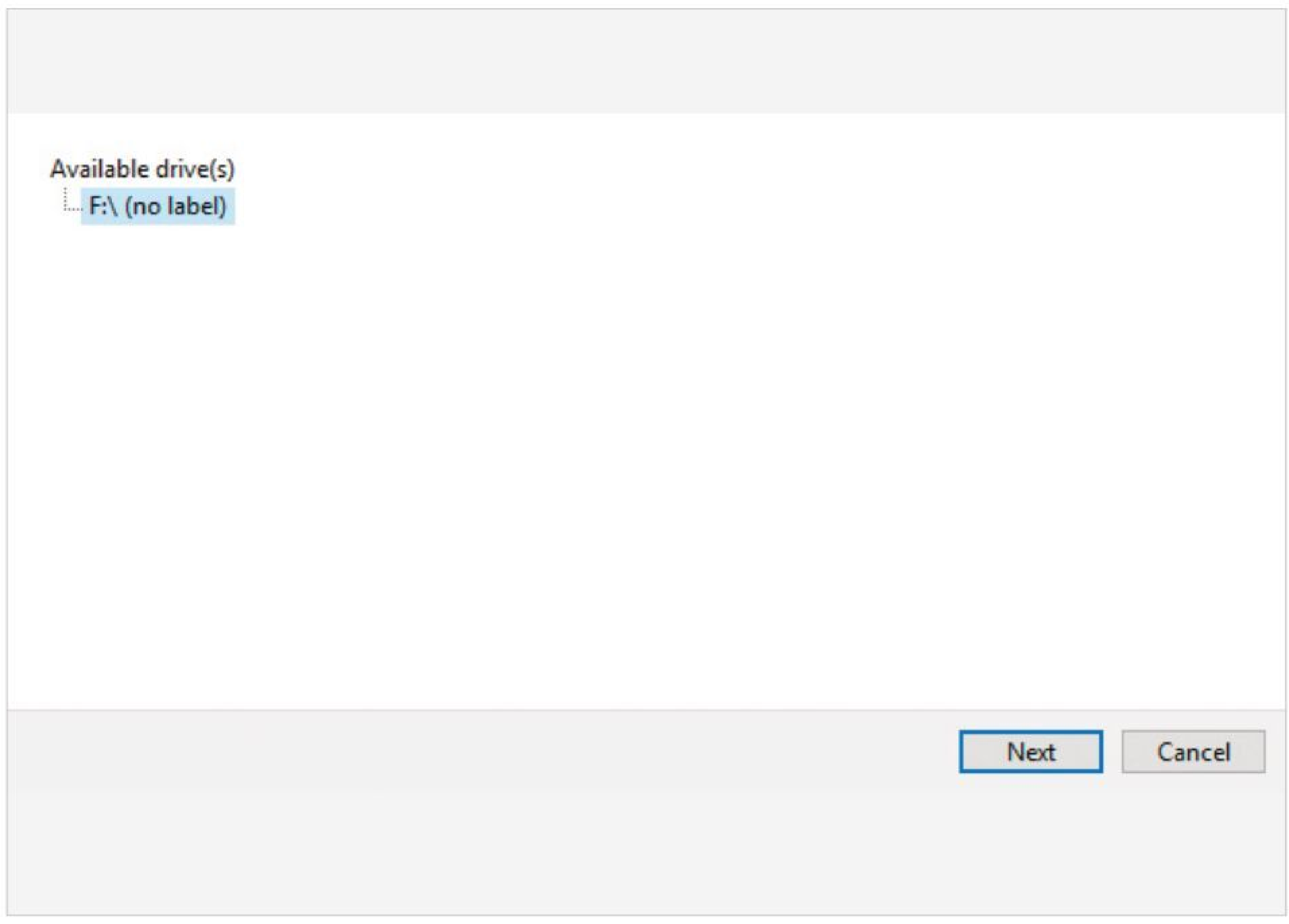


Select the USB flash drive

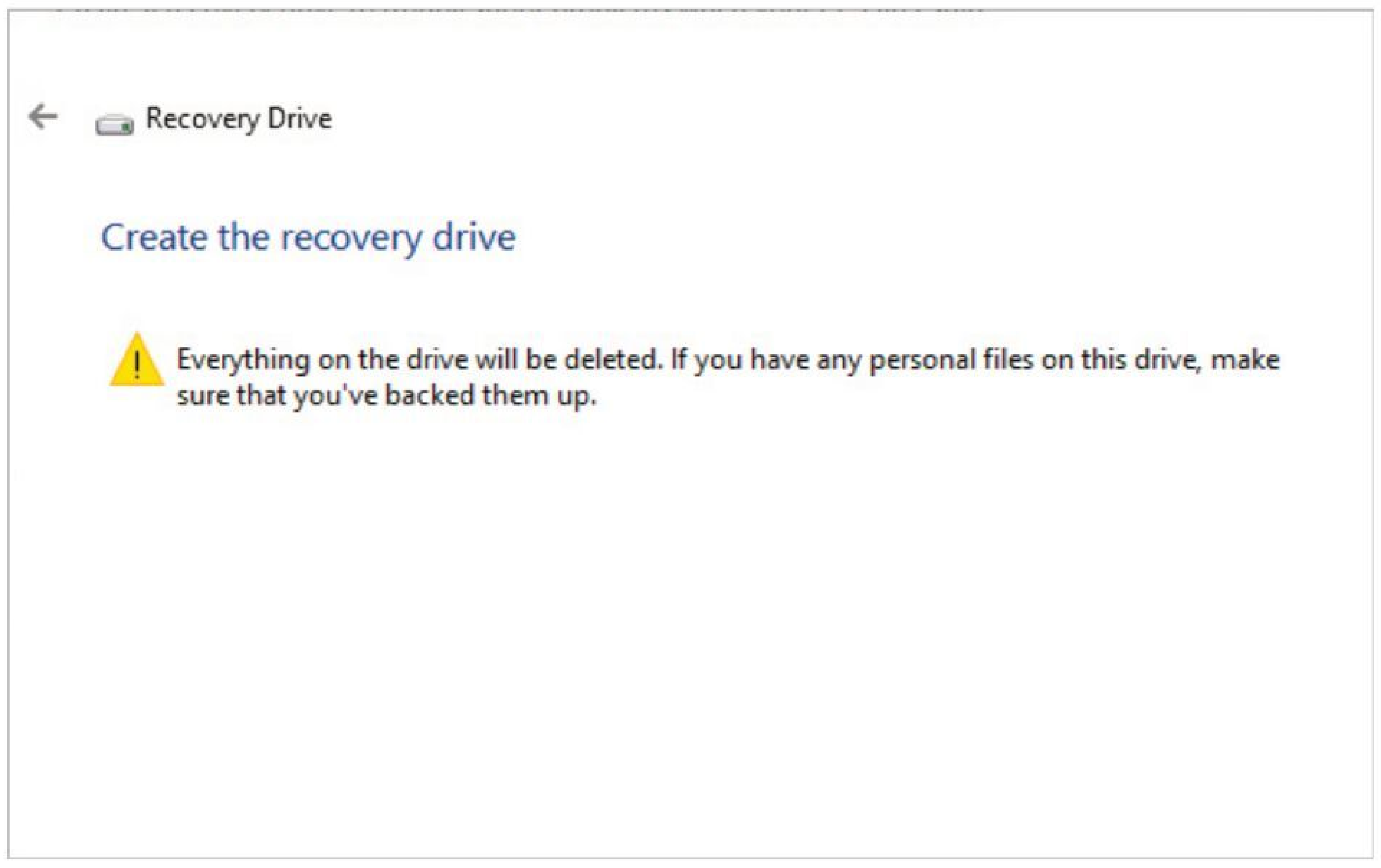
The drive must be able to hold at least 8 GB, and everything on the drive will be deleted.

Available drive(s)
F:\ (no label)

STEP 4 In the example we have here, there's just one possible location, the F:\ drive. If you have more than one possible destination available, make sure that you're selecting the correct USB drive for your recovery drive. When you're ready, click on the Next button.


Available drive(s)
F:\ (no label)

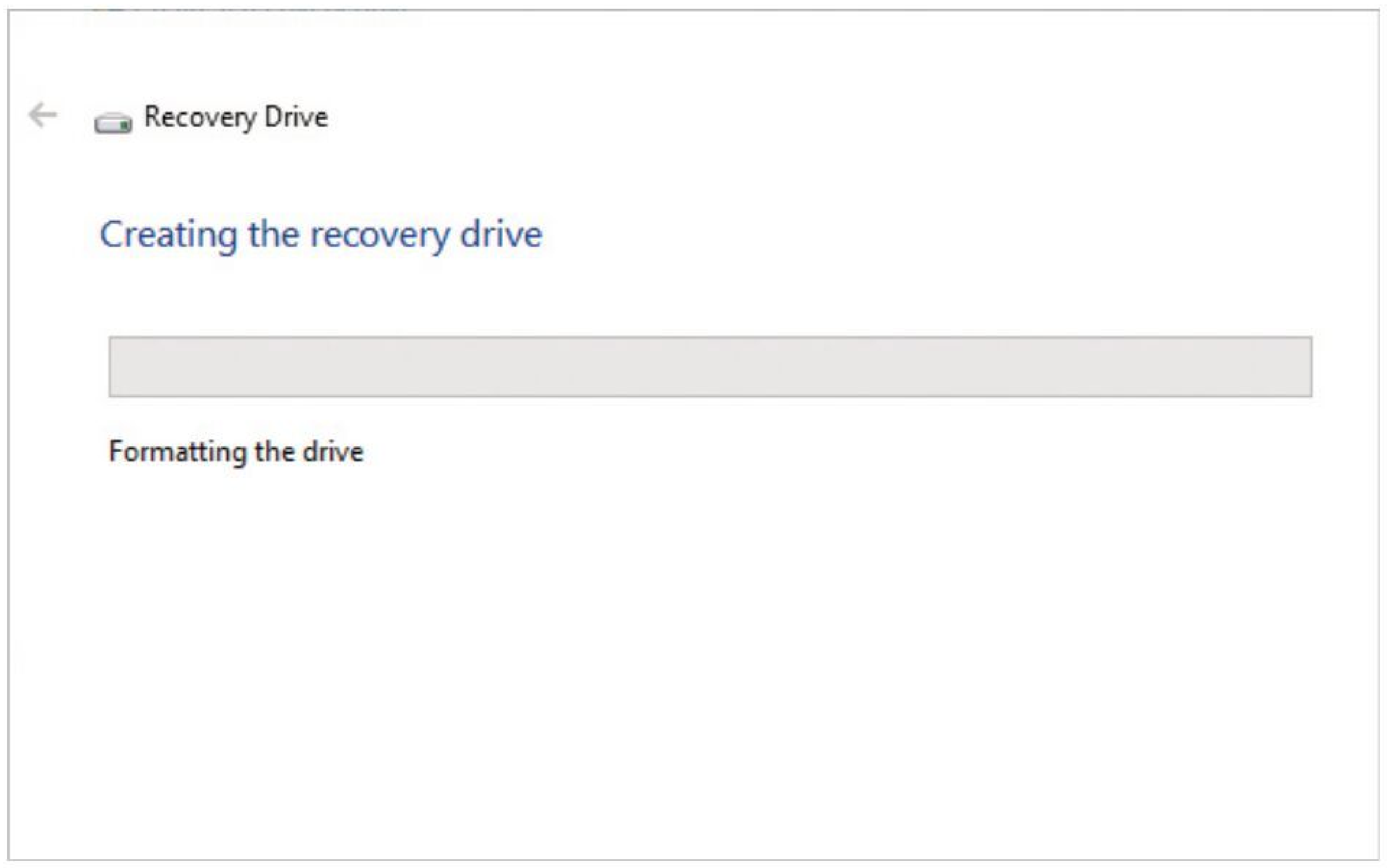
STEP 5 Before committing to creating the recovery drive, Windows will offer one final warning. Remember, everything that's currently on the USB stick you chose as the recovery drive will be erased during the process of creating the drive. If you have any files stored on it, make sure they're backed up to another location.


Recovery Drive

Create the recovery drive

Everything on the drive will be deleted. If you have any personal files on this drive, make sure that you've backed them up.

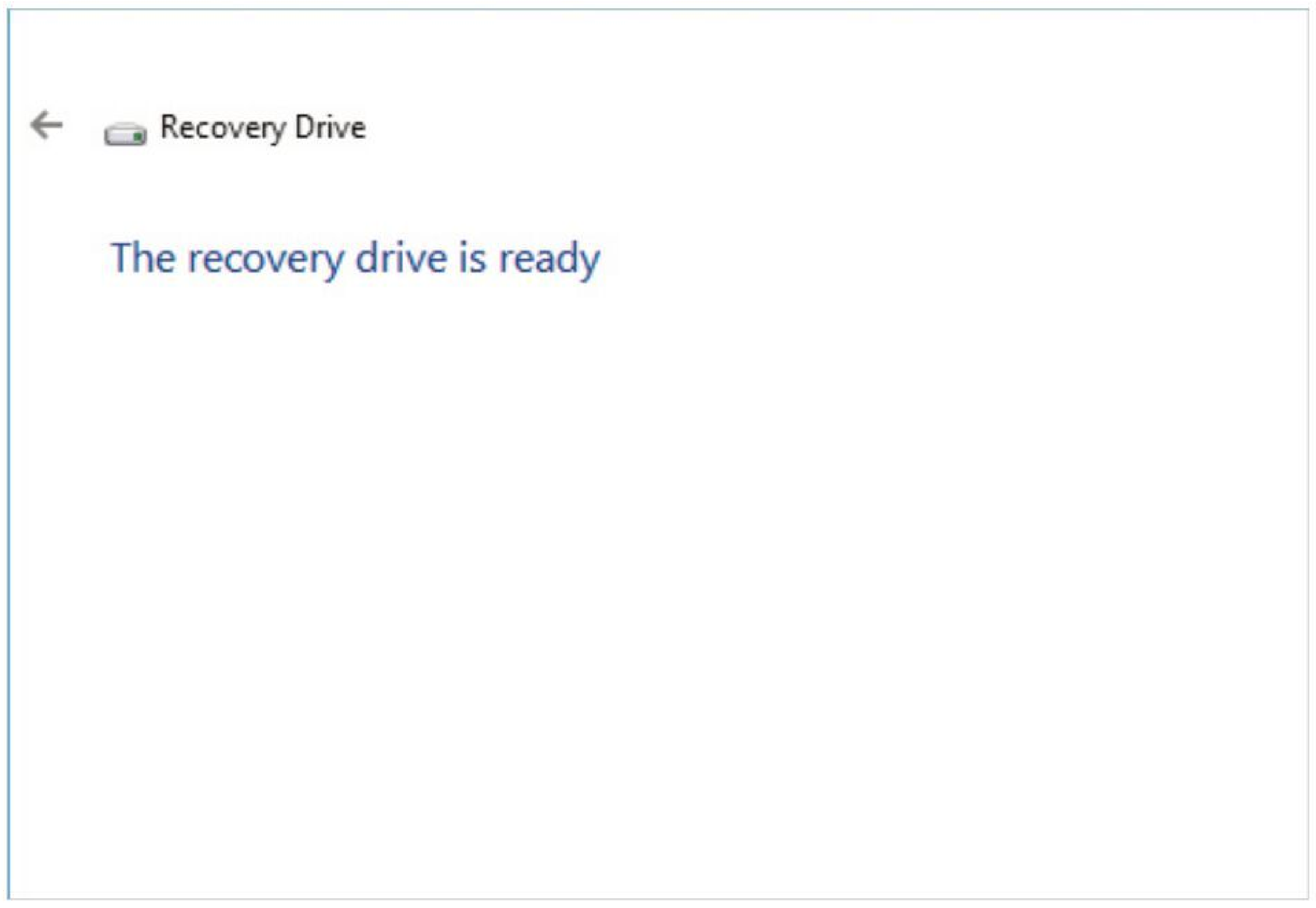
STEP 6 When you're ready click on the Create button to start the process. It may take some time, depending on the speed of the USB stick used, as Windows prepares, formats and copies the utilities and files over to the USB recovery drive.


Recovery Drive

Creating the recovery drive

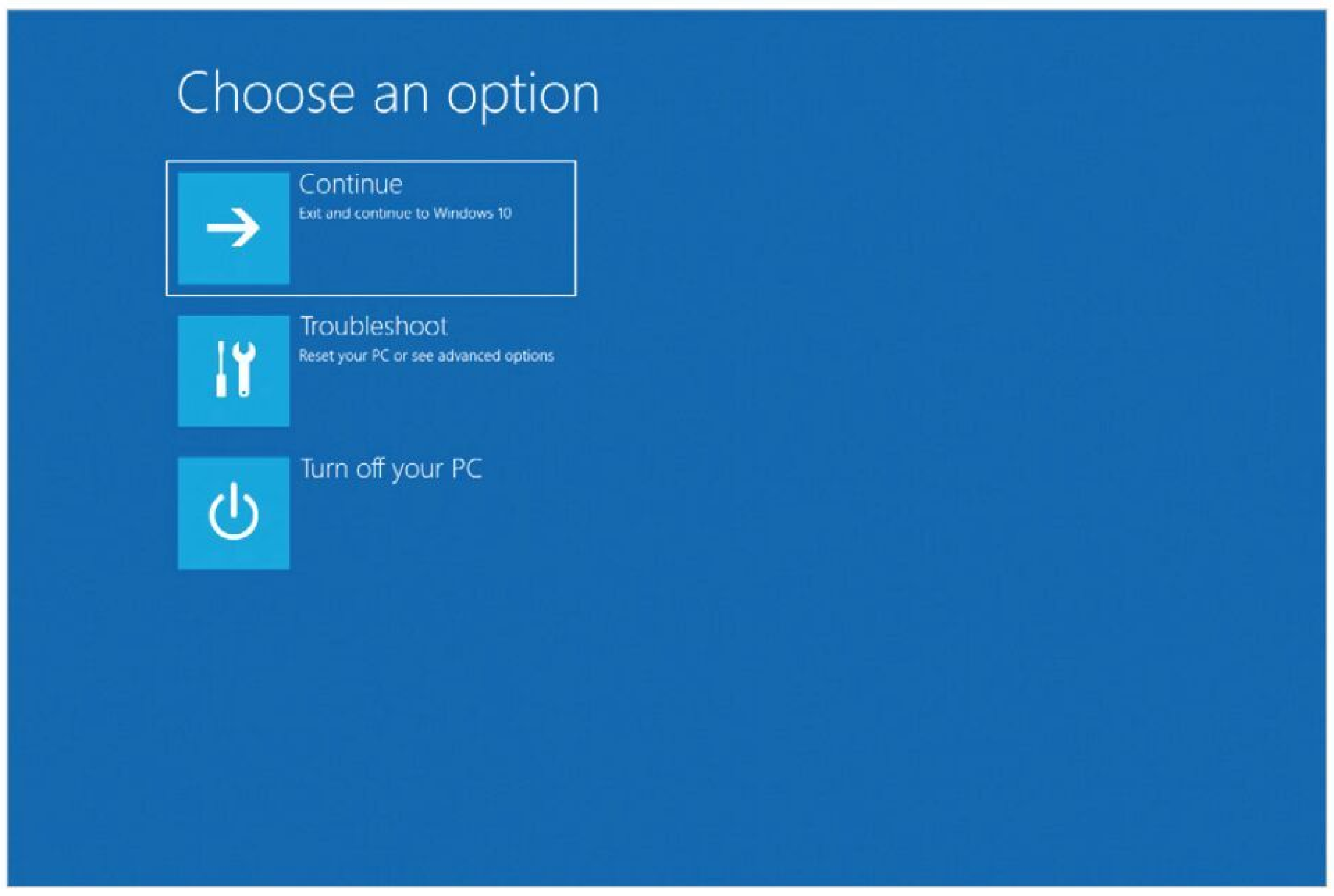
Formatting the drive

STEP 7 When the process is complete, you receive a recovery drive is ready message. The only option available to you is to click the Finish button. This will close the recovery drive window and return you to the Recovery console.

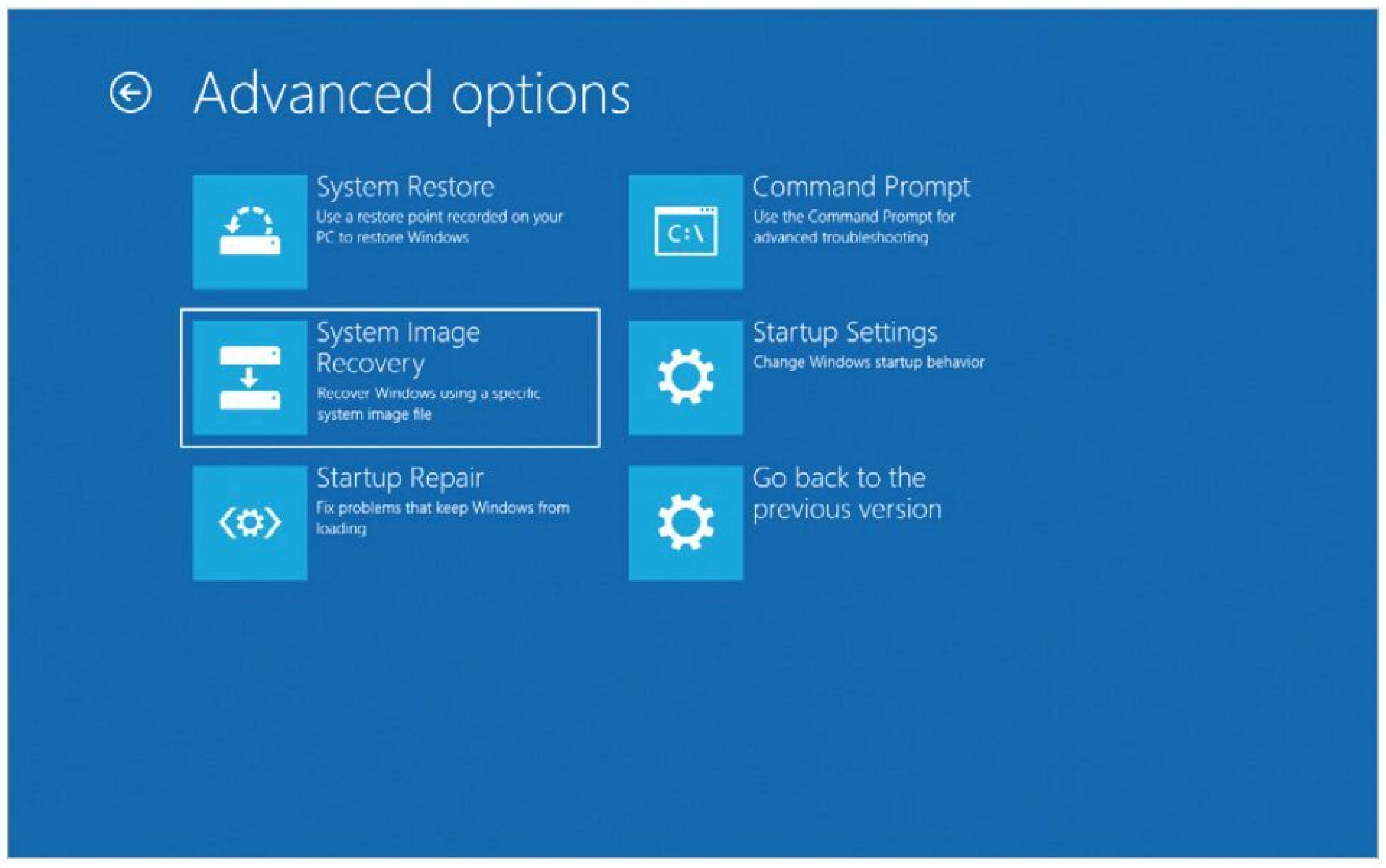

Recovery Drive

The recovery drive is ready

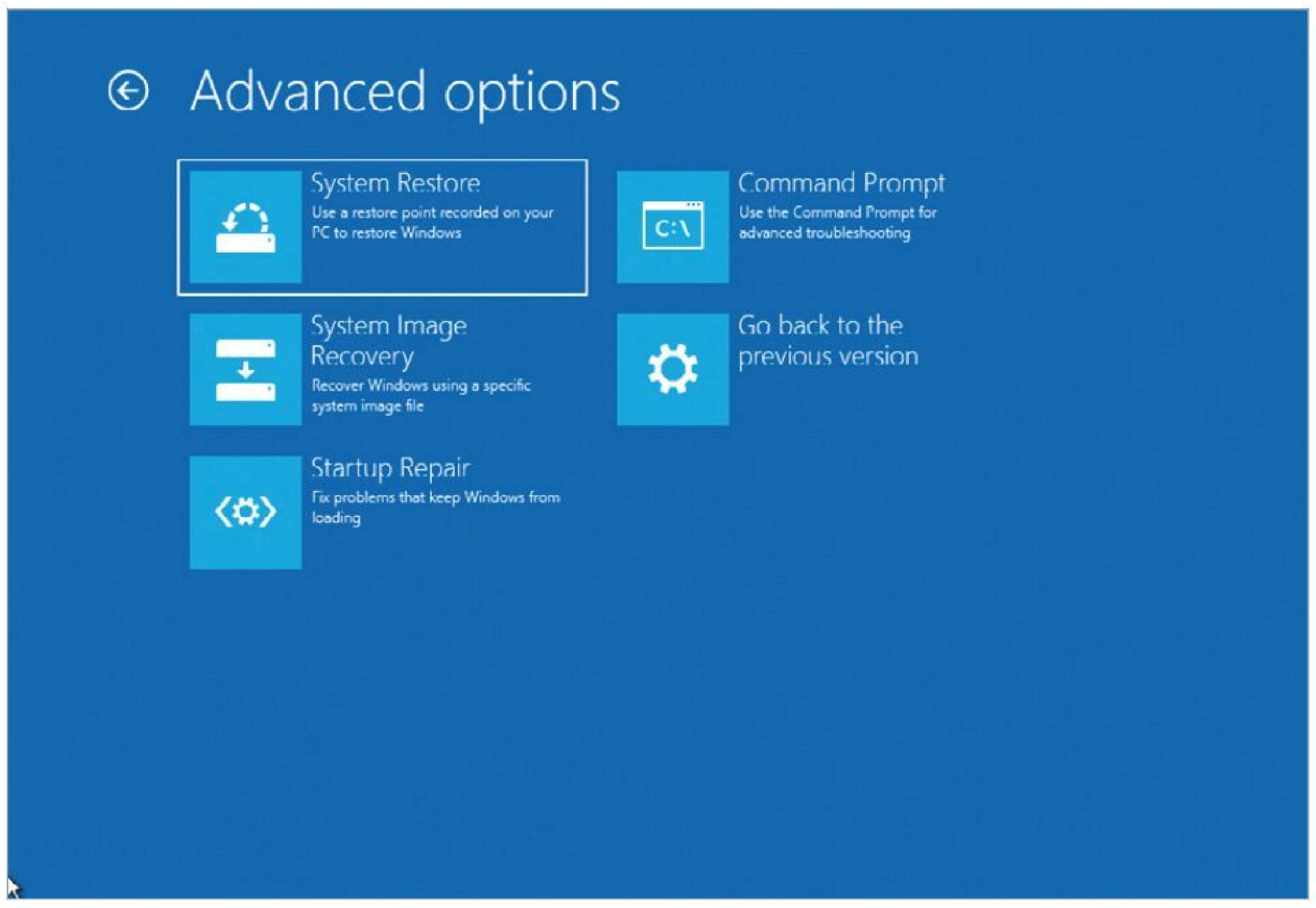
STEP 8 Store the drive in a safe place, as it can restore vital system files should anything ever go wrong with your system and leave it unable to boot. Should something go wrong, you see the Windows 10 safe mode boot options when you try and power up your computer.


Choose an option
Continue
Exit and continue to Windows 10
Troubleshoot
Reset your PC or see advanced options
Turn off your PC

STEP 9 From the safe mode boot options, choose the Troubleshoot tile followed by Advanced Options. From there you can choose the System Restore and System Image Recovery options along with your rescue drive to help you recover Windows.


Advanced options
System Restore
Use a restore point recorded on your PC to restore Windows
Command Prompt
Use the Command Prompt for advanced troubleshooting
System Image Recovery
Recover Windows using a specific system image file
Startup Settings
Change Windows startup behavior
Startup Repair
Fix problems that keep Windows from loading
Go back to the previous version

STEP 10 Alternatively, set the BIOS to boot to the newly created recovery drive and follow the onscreen instructions to launch the recovery method. Start by choosing your language, then select the Troubleshoot option and then opt for one of several recovery options.


Advanced options
System Restore
Use a restore point recorded on your PC to restore Windows
Command Prompt
Use the Command Prompt for advanced troubleshooting
System Image Recovery
Recover Windows using a specific system image file
Go back to the previous version
Startup Repair
Fix problems that keep Windows from loading

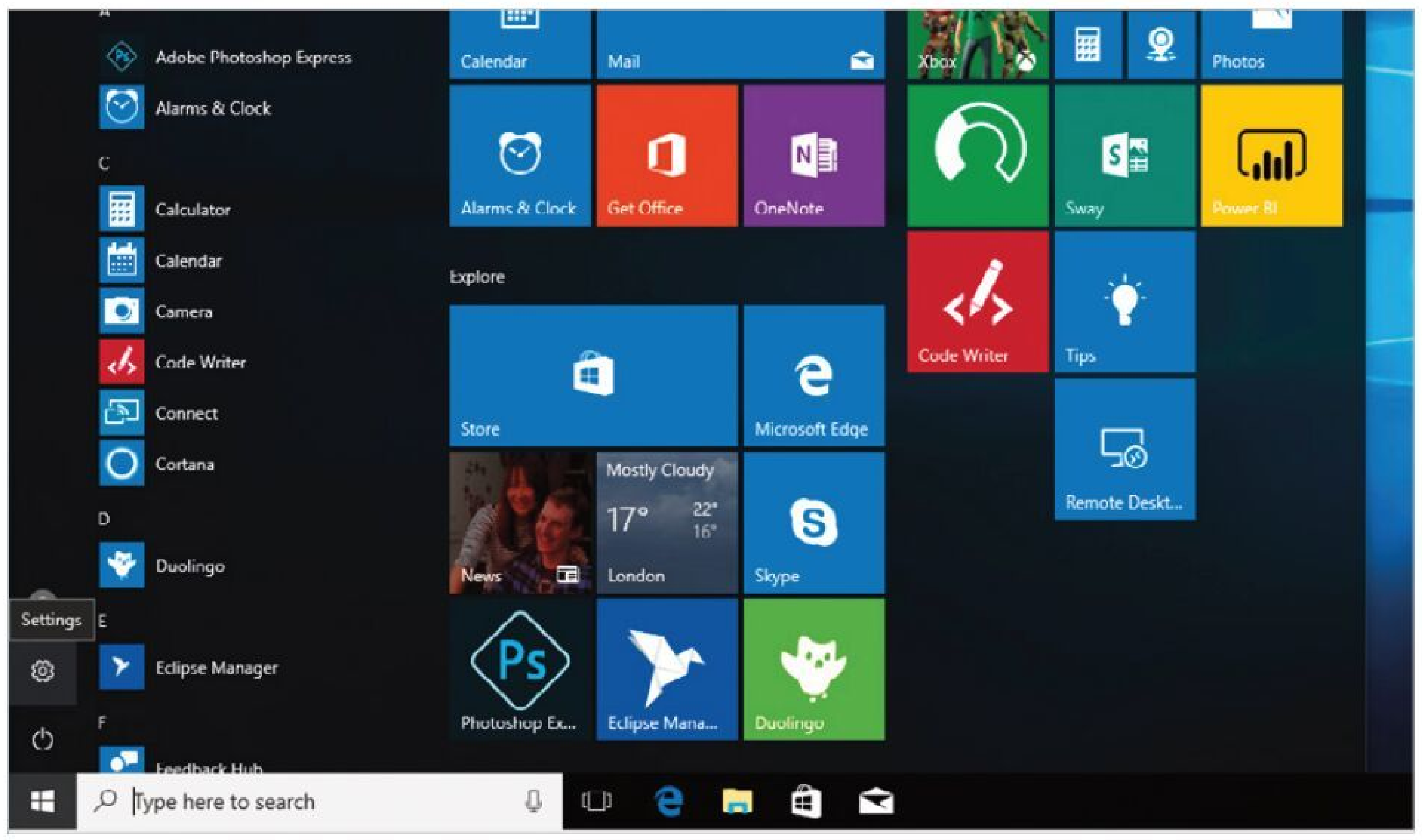
How to Back Up Windows 10

Even with the greatest possible cyber protection in the world guarding your computer, there's still a chance something could go wrong. It might not even be malware-related; a broken hard drive or other component can cause as much grief. Therefore, you need a good backup.

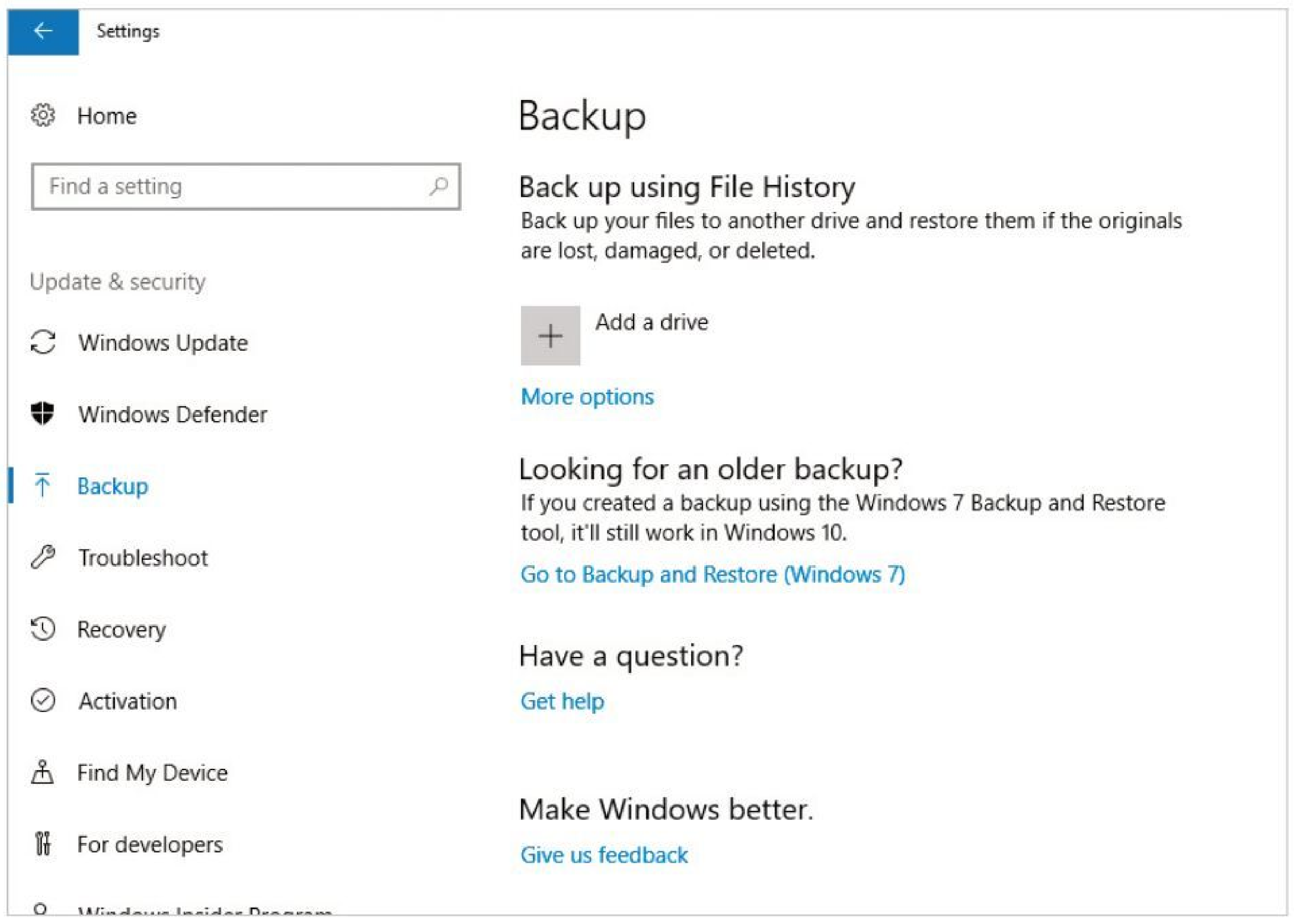
Backing Up

Computers are unpredictable beasts, so you need to make sure that all your files and important data are securely backed up and more importantly, you're able to restore them easily. Thankfully, it's a straightforward process.

STEP 1 Windows has, since its early days, featured some form of backup tool. Windows 10 was launched with the File History backup tool, which is a simple to use tool to ensure stable and regular backups of important files are made. Start by clicking on the Windows Start button and selecting Settings from the menu.


Adobe Photoshop Express
Alarms & Clock
C
Calculator
Calendar
Camera
Code Writer
Connect
Cortana
D
Duolingo
Settings
E
Eclipse Manager
F
Feedback Hub
Calendar
Mail
Xbox
Photos
Alarms & Clock
Get Office
OneNote
Sway
Power BI
Explore
Code Writer
Tips
Store
Microsoft Edge
Remote Deskt...
Mostly Cloudy
17°
22°
16°
London
News
Skype
Photoshop Ex...
Eclipse Mana...
Duolingo
Type here to search

STEP 2 Once in the Settings console, click on the Update & Security icon, followed by the Backup option from the menu on the left. You can see a number of possible options before you: Add a Drive, More options, Go to Backup and Restore (Windows 7), along with help and feedback links.


Settings
Home
Find a setting
Update & security
Windows Update
Windows Defender
Backup
Troubleshoot
Recovery
Activation
Find My Device
For developers
Windows Insider Program

Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Add a drive
More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

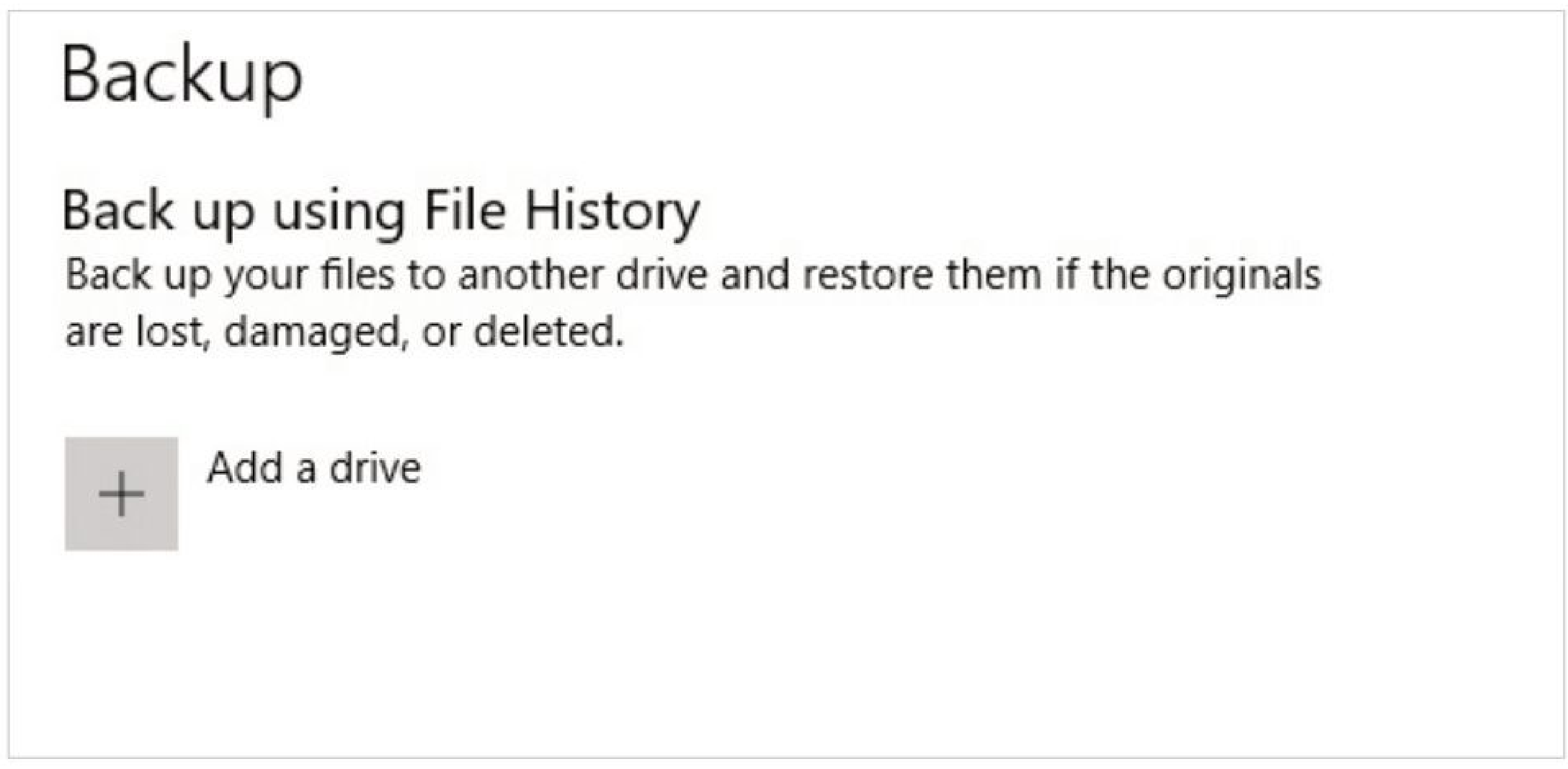
Have a question?

Get help

Make Windows better.

Give us feedback

STEP 3 Ideally you need to insert a reasonably sized USB stick or use a second hard drive in your computer. If you have a USB stick, insert it now, or if you own a second hard drive power off the computer and install it and boot back into Windows 10. Once done, click the Add a Drive icon.

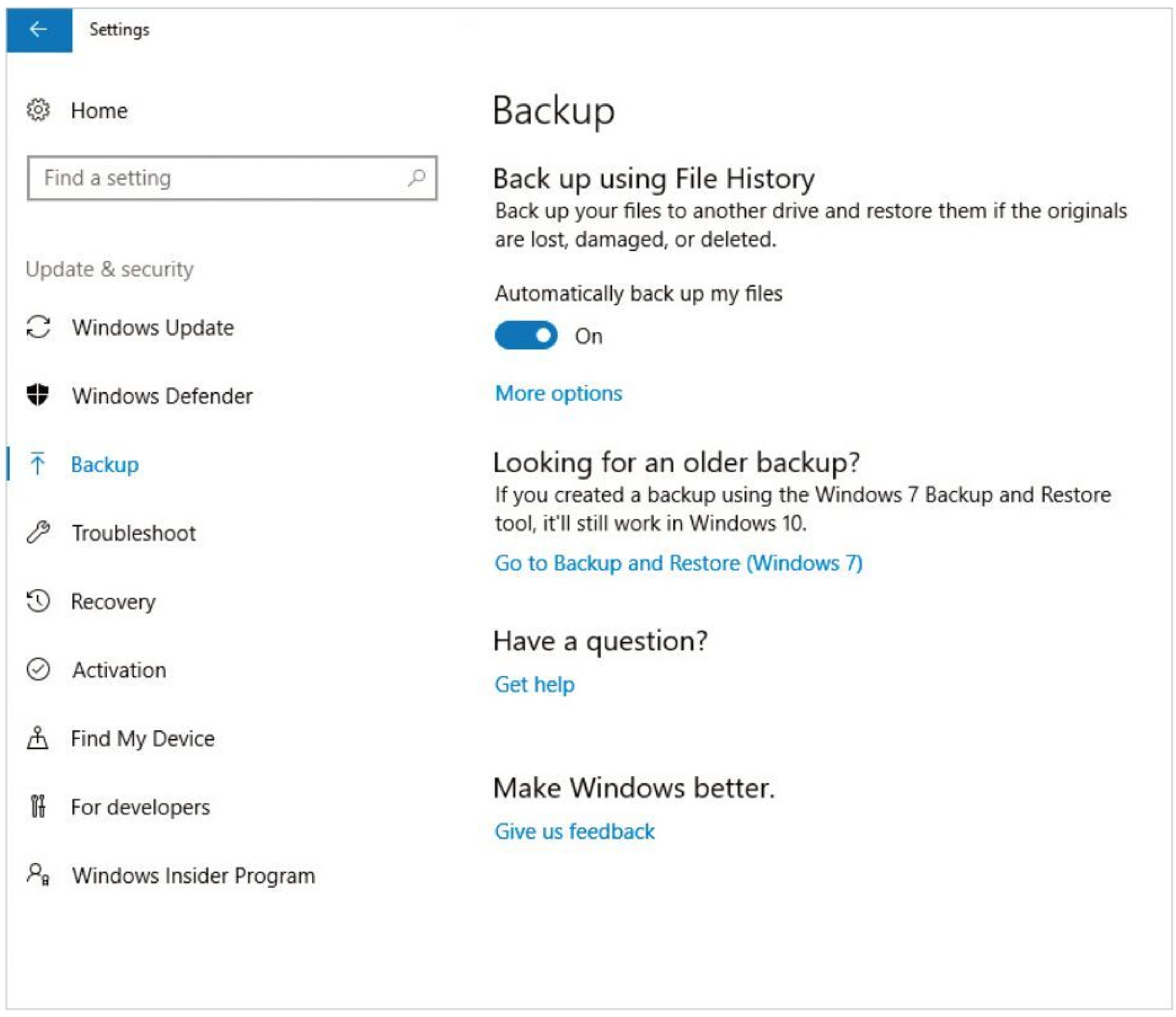


Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

STEP 4 Windows will search for any capable drives on to which it's able to back up your files. When your drive or USB device is displayed, click the drive link. Notice that an 'Automatically back up my files' switch button has appeared where Add a drive once was.


Settings
Home
Find a setting
Update & security
Windows Update
Windows Defender
Backup
Troubleshoot
Recovery
Activation
Find My Device
For developers
Windows Insider Program

Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Automatically back up my files: On

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

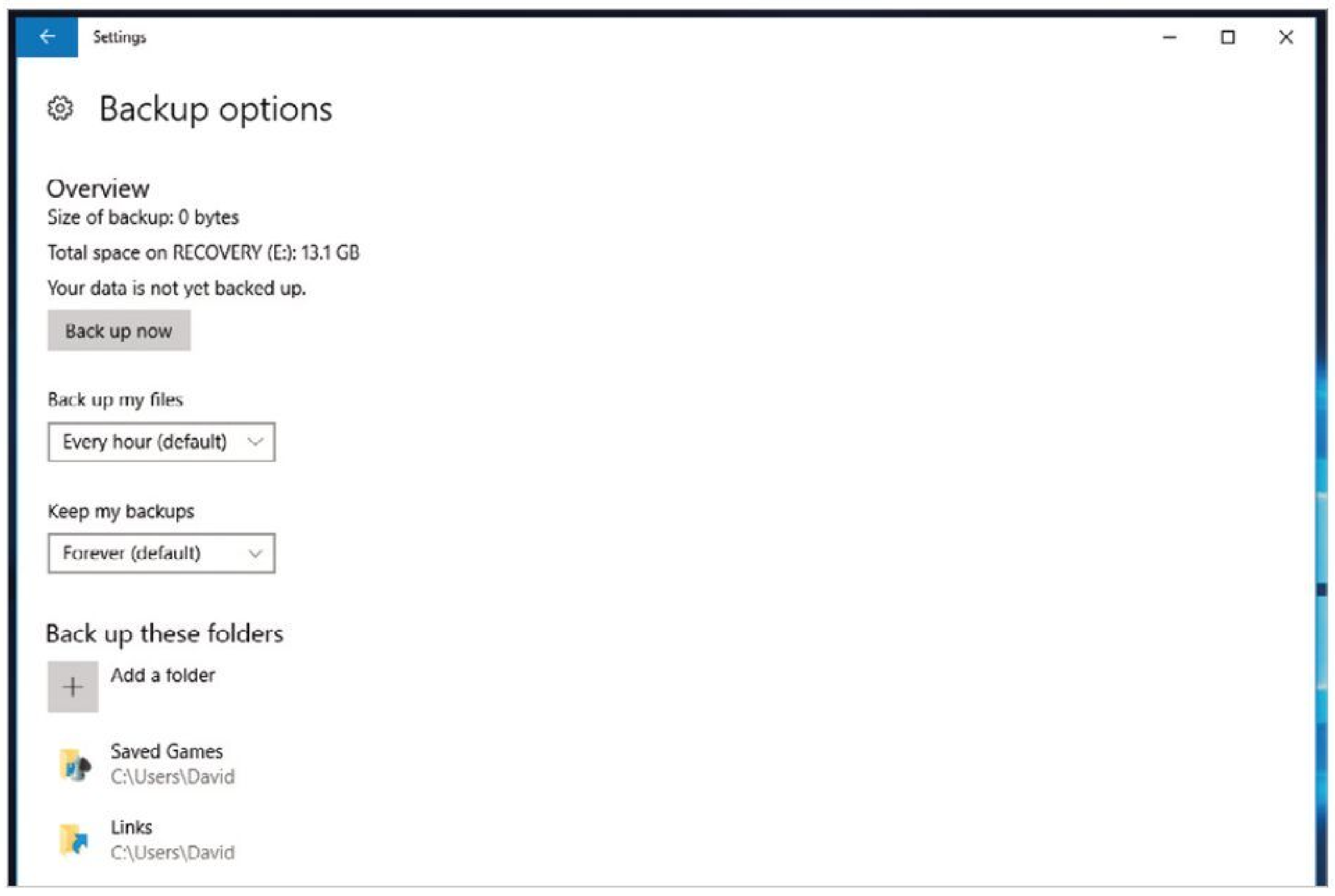
Have a question?

Get help

Make Windows better.

Give us feedback

STEP 5 From here, click on the More Options link that's under the switch button, this will open the Backup Options console. This section details the backup schedule, the location and which folders will be included in the backup; and for how long Windows will retain your backed up files.


Settings
Back up now
Add a folder

Backup options

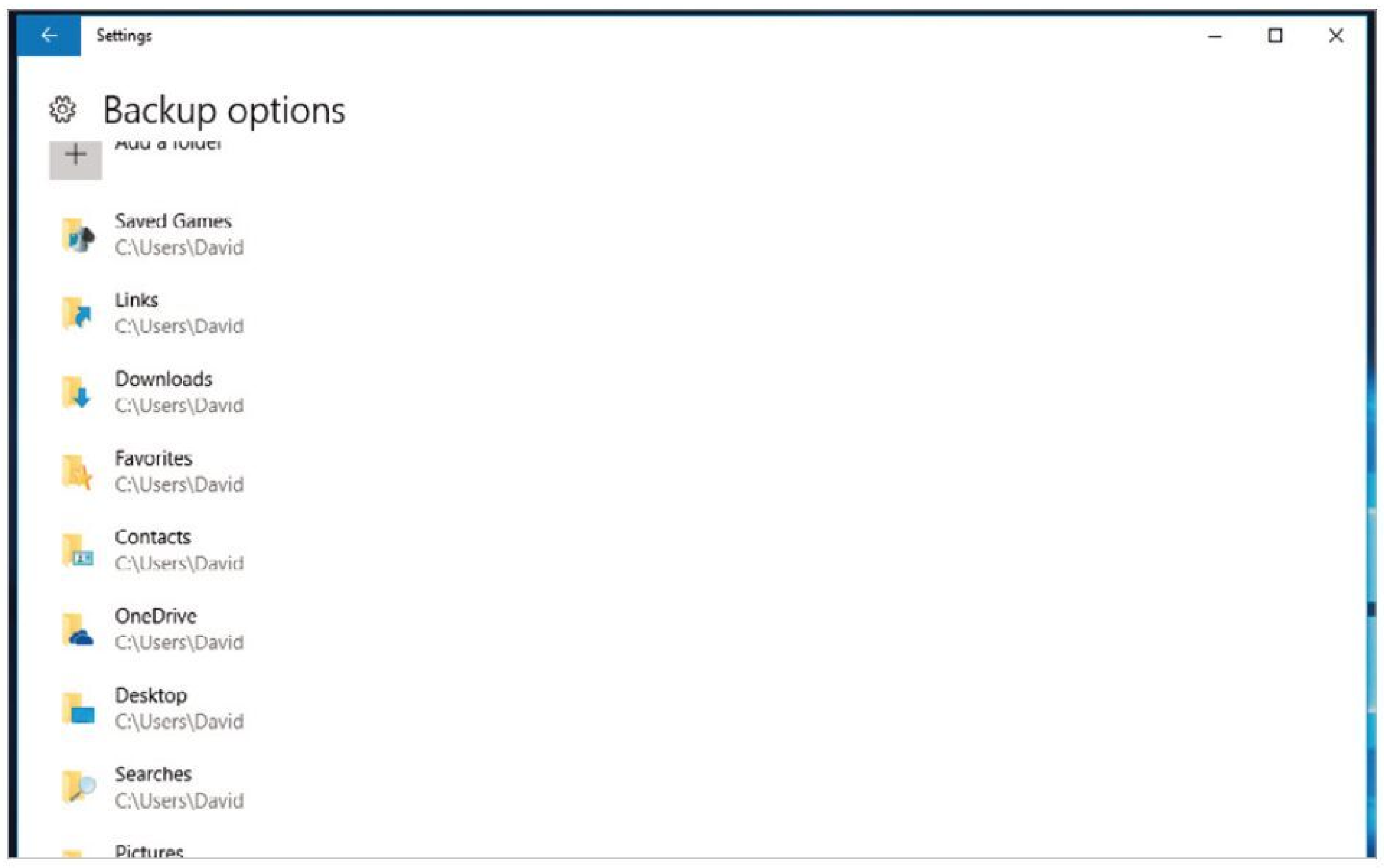
Overview
Size of backup: 0 bytes
Total space on RECOVERY (E:): 13.1 GB
Your data is not yet backed up.

Back up my files: Every hour (default)

Keep my backups: Forever (default)

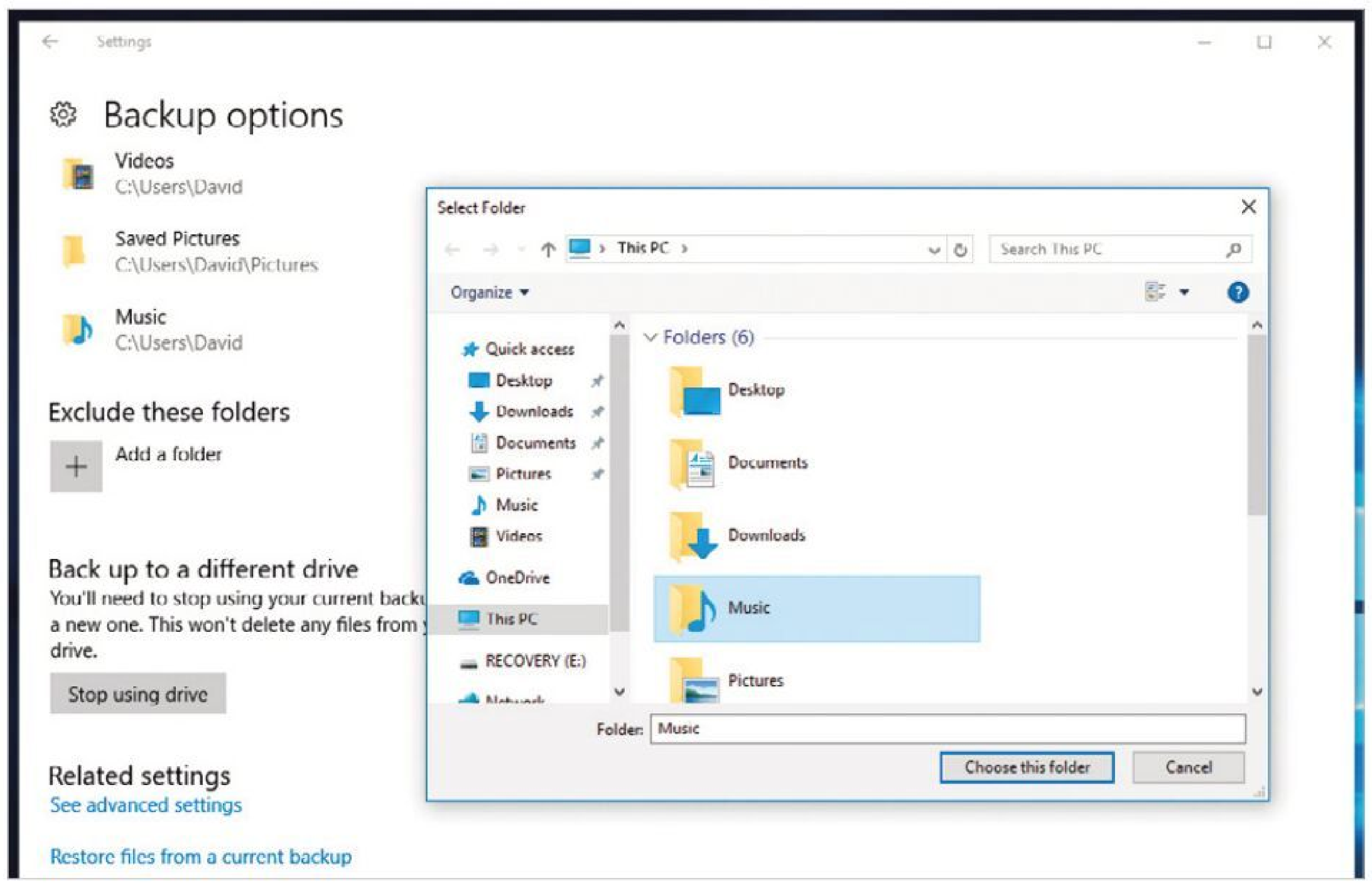
Back up these folders
Saved Games C:\Users\David
Links C:\Users\David

STEP 6 If you scroll down through the Backup Options console, you can see that the entirety of your user folder within Windows 10 has been added by default. This includes the Music and Videos folders, as well as Searches, Camera Roll, Contacts, Favourites and so on.


Settings
Add a folder

Backup options
Saved Games C:\Users\David
Links C:\Users\David
Downloads C:\Users\David
Favorites C:\Users\David
Contacts C:\Users\David
OneDrive C:\Users\David
Desktop C:\Users\David
Searches C:\Users\David
Pictures

STEP 7 At the bottom of the console window you have the options to stop using the selected drive and to Exclude any folders from the default. If you don't want to back up folders for Music, Videos etc., click Add a folder on the Exclude these folders icon, then pick the folder to exclude and click the Choose this folder button.


Settings
Add a folder
Stop using drive
Select Folder
This PC
Search This PC
Organize
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
RECOVERY (E:)
Network
Folders (6)
Desktop
Documents
Downloads
Music
Pictures
Choose this folder
Cancel

Backup options
Videos C:\Users\David
Saved Pictures C:\Users\David\Pictures
Music C:\Users\David

Exclude these folders

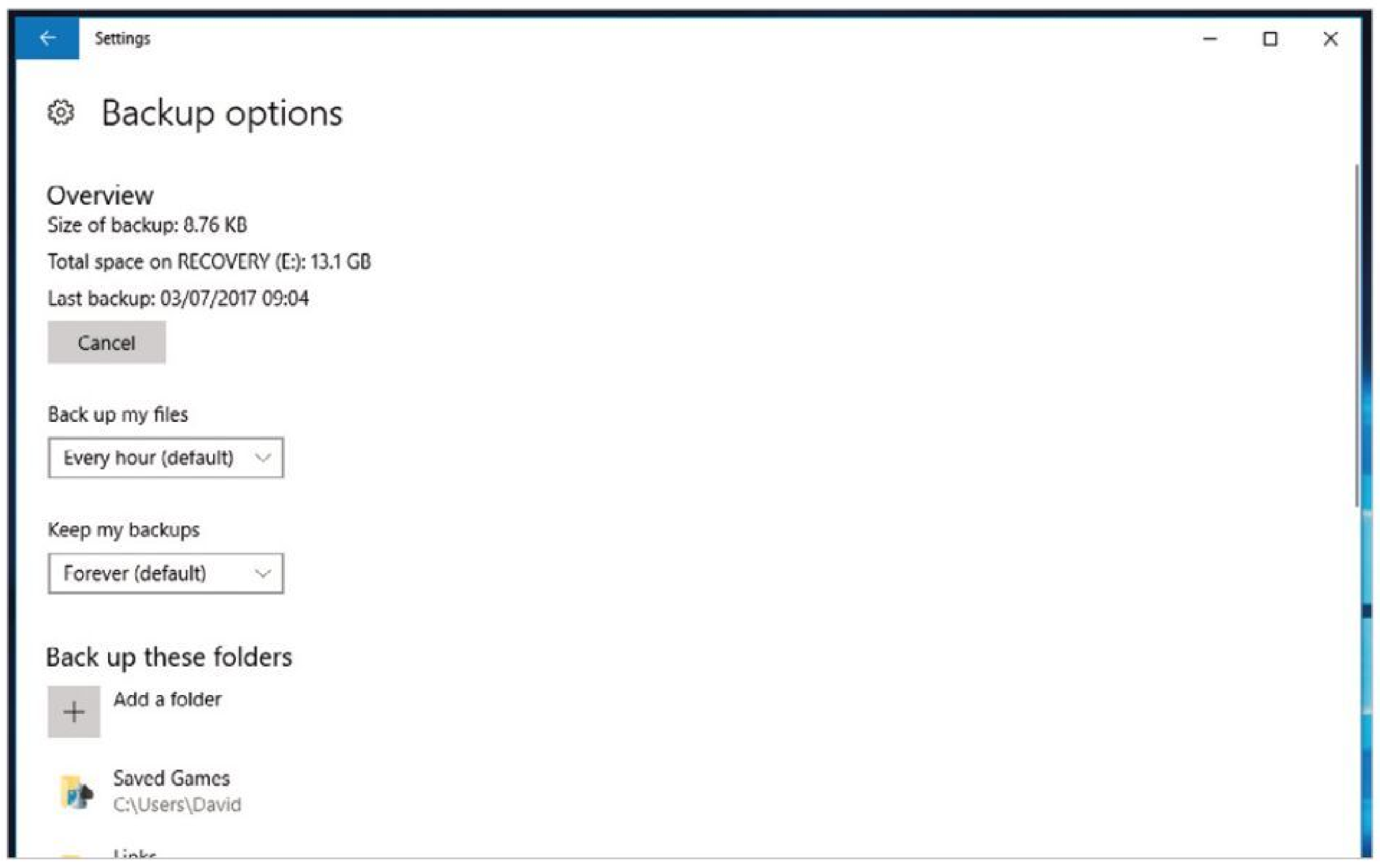
Back up to a different drive
You'll need to stop using your current backu
a new one. This won't delete any files from y
drive.

Related settings
See advanced settings

Restore files from a current backup

Folder: Music

STEP 8 When you're ready to start backing up, you can click the Back up now button to the top of the Backup Option console window. Alternatively, you can wait for an hour when the default schedule kicks in. Obviously, depending on the size of the files within your backup folders this could take some time.


Settings
Cancel
Add a folder

Backup options

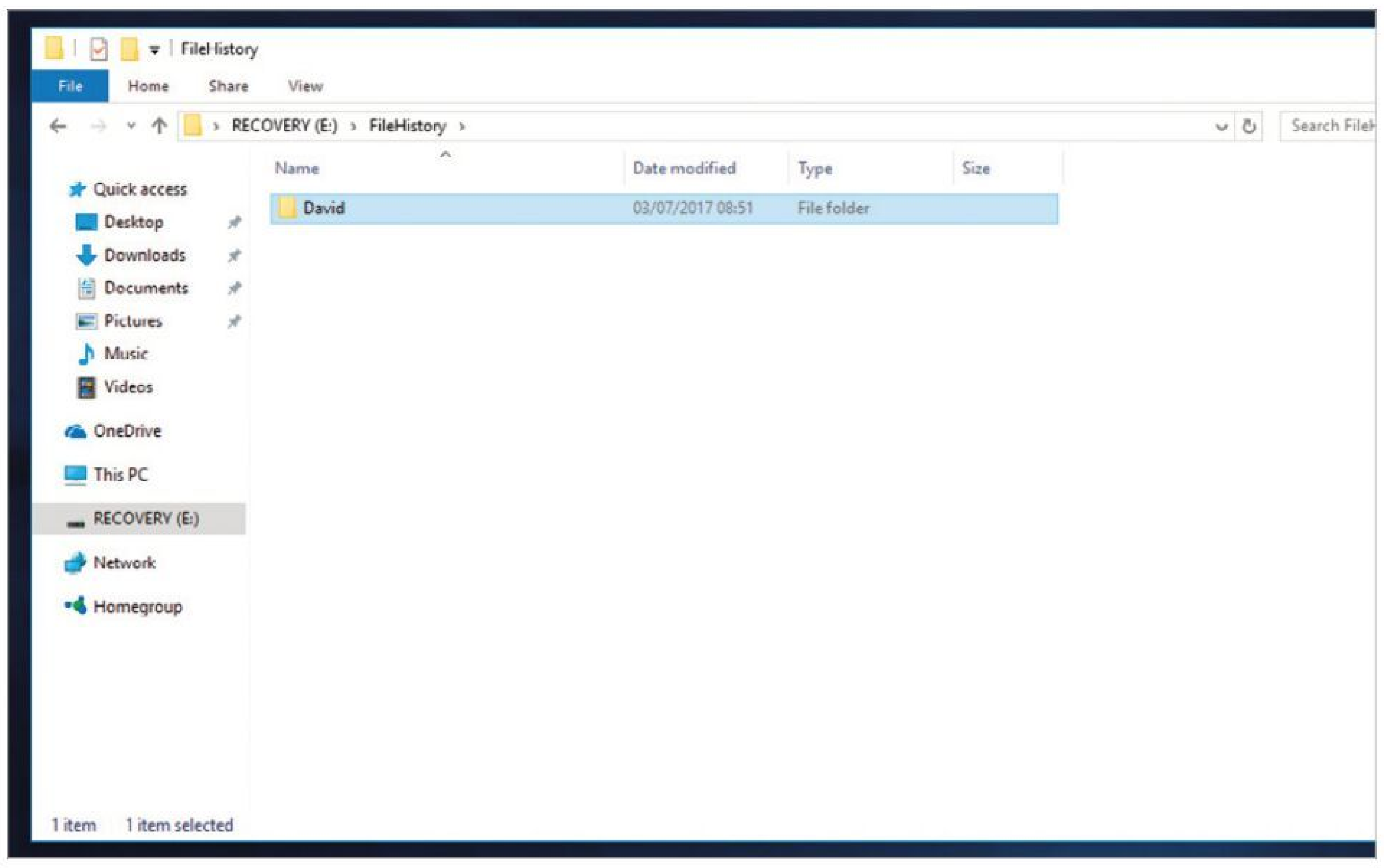
Overview
Size of backup: 8.76 KB
Total space on RECOVERY (E:): 13.1 GB
Last backup: 03/07/2017 09:04

Back up my files: Every hour (default)

Keep my backups: Forever (default)

Back up these folders
Saved Games C:\Users\David

STEP 9 The backed up files will be stored on the chosen backup drive, within a folder called FileHistory. Inside that folder will be the specific user folder, so if you use File History backups for more than one user, their user names will be listed here too.

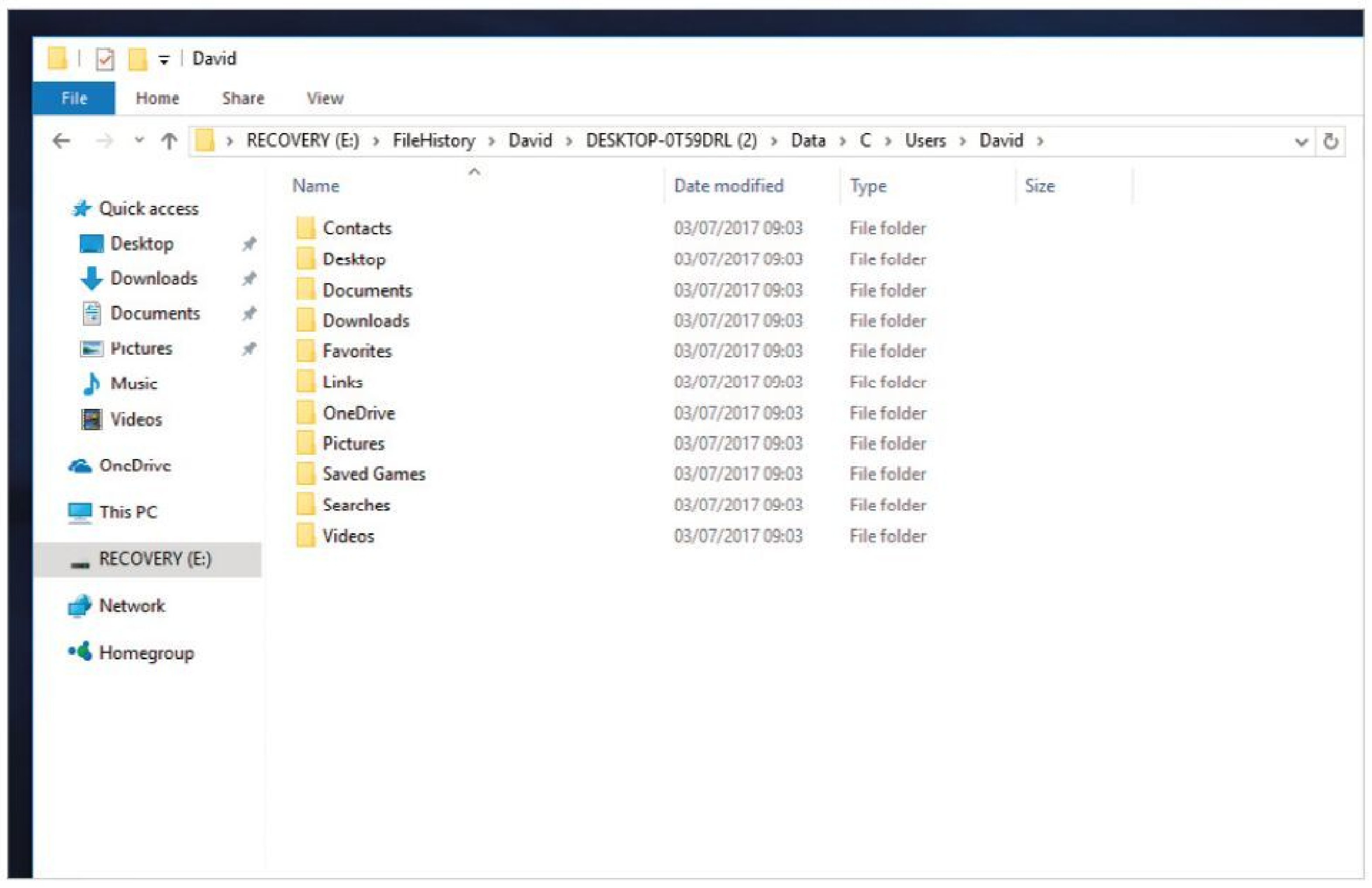

FileHistory
File
Home
Share
View
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
RECOVERY (E:)
Network
Homegroup

RECOVERY (E:) › FileHistory ›

Name	Date modified	Type	Size
David	03/07/2017 08:51	File folder	

1 item 1 item selected

STEP 10 Drilling deeper into the folder layers reveals more default folders, containing important XML data that Windows uses to store the chosen options. You can find the actual files that have been backed up in the Data folder, laid out in the same folder structure as on your system, i.e. C > Users > Name > Documents etc.


David
File
Home
Share
View
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
RECOVERY (E:)
Network
Homegroup

RECOVERY (E:) › FileHistory › David › DESKTOP-0T59DRL (2) › Data › C › Users › David ›

Name	Date modified	Type	Size
Contacts	03/07/2017 09:03	File folder	
Desktop	03/07/2017 09:03	File folder	
Documents	03/07/2017 09:03	File folder	
Downloads	03/07/2017 09:03	File folder	
Favorites	03/07/2017 09:03	File folder	
Links	03/07/2017 09:03	File folder	
OneDrive	03/07/2017 09:03	File folder	
Pictures	03/07/2017 09:03	File folder	
Saved Games	03/07/2017 09:03	File folder	
Searches	03/07/2017 09:03	File folder	
Videos	03/07/2017 09:03	File folder	

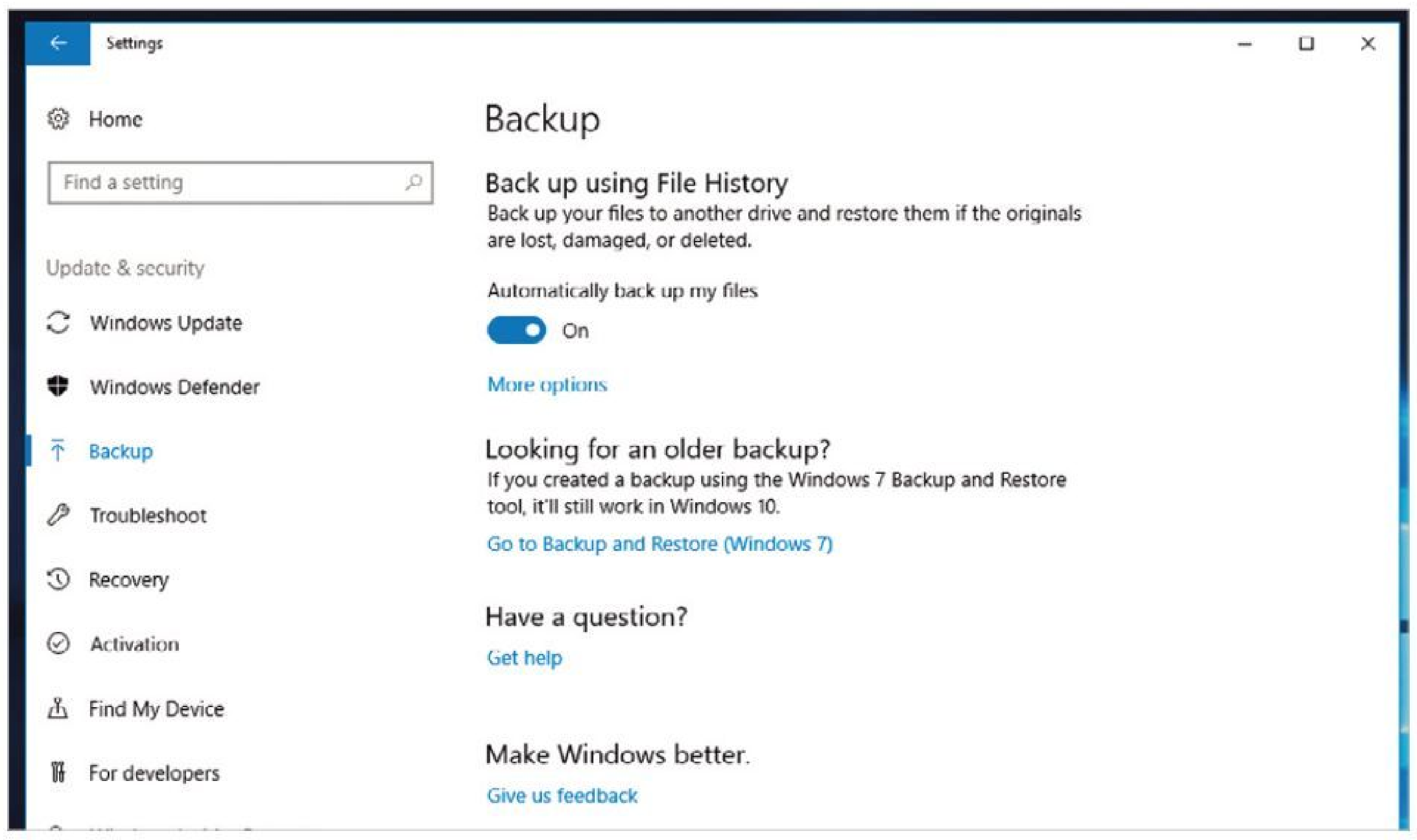
How to Create a Windows 10 System Image

Backing up your files is perfectly fine but in the event of having to wipe your hard drive and start again, getting everything back in order can be time consuming. However, creating a system image means you can almost instantly restore the entire system without needing to rebuild Windows.

System Imaging

A system image works in much the same way as the VirtualBox Snapshots. You're essentially taking a snapshot of your entire system, which can then be restored quickly. Saving you having to reinstall Windows 10, all your programs and data.

STEP 1 To begin, click on the Windows Start button and once more navigate to Settings > Update & Security > Backup. From within the Backup console window, where you were in the previous tutorial, click on the Go to Backup and Restore (Windows 7) link under the Looking for an older backup section.


Settings
Home
Find a setting
Update & security
Windows Update
Windows Defender
Backup
Troubleshoot
Recovery
Activation
Find My Device
For developers
More options
Go to Backup and Restore (Windows 7)
Get help
Give us feedback

Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Automatically back up my files

On

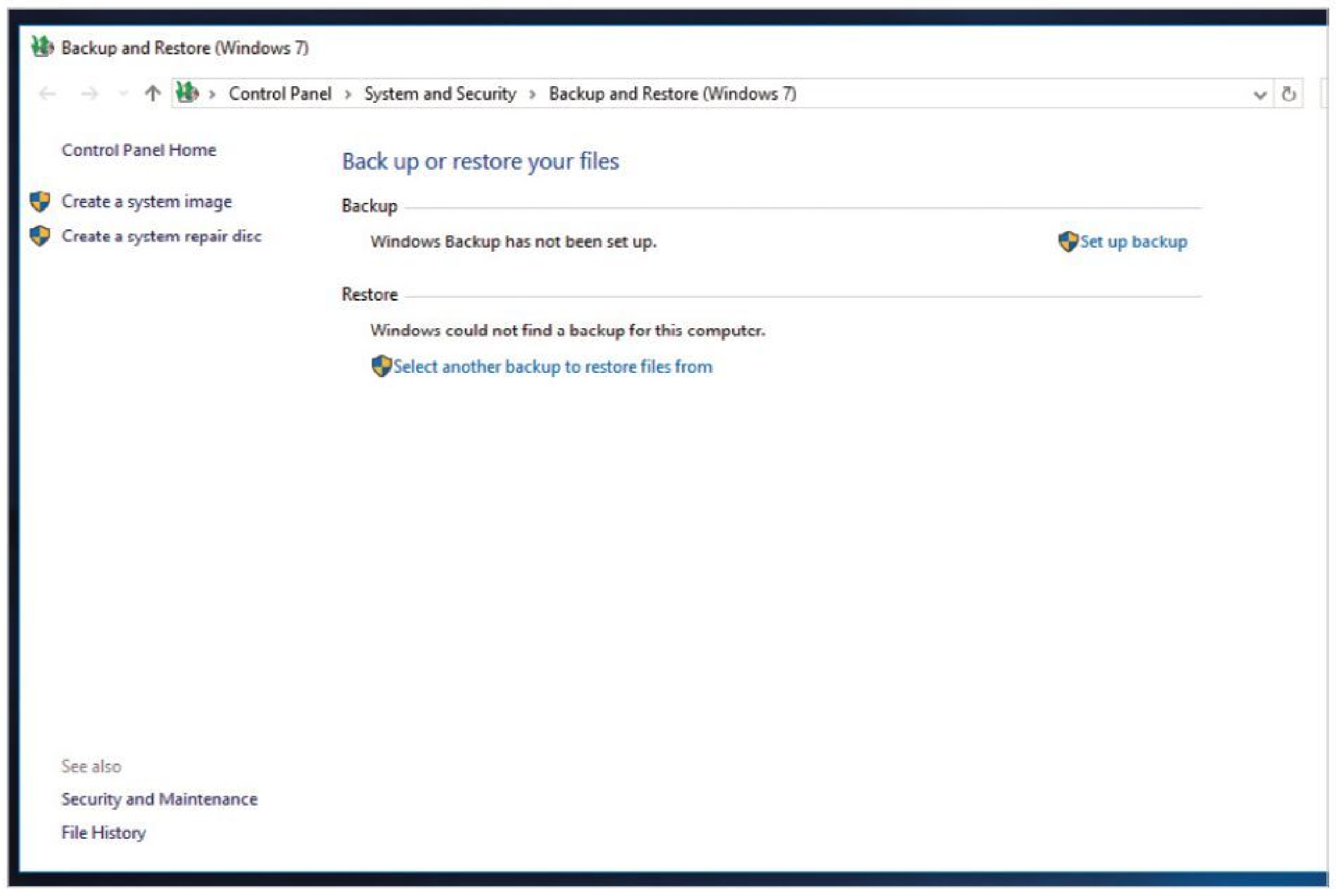
Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Have a question?

Make Windows better.

STEP 2 This will launch a new window, the Backup and Restore (Windows 7) console. Microsoft has kept this feature intact through Windows 8.1 and 10 purely due to compatibility support for backups done under older versions of the OS. To the left there are two links, click on the Create a system image link.


Backup and Restore (Windows 7)
Control Panel > System and Security > Backup and Restore (Windows 7)
Control Panel Home
Create a system image
Create a system repair disc
Set up backup
Select another backup to restore files from
See also
Security and Maintenance
File History

Back up or restore your files

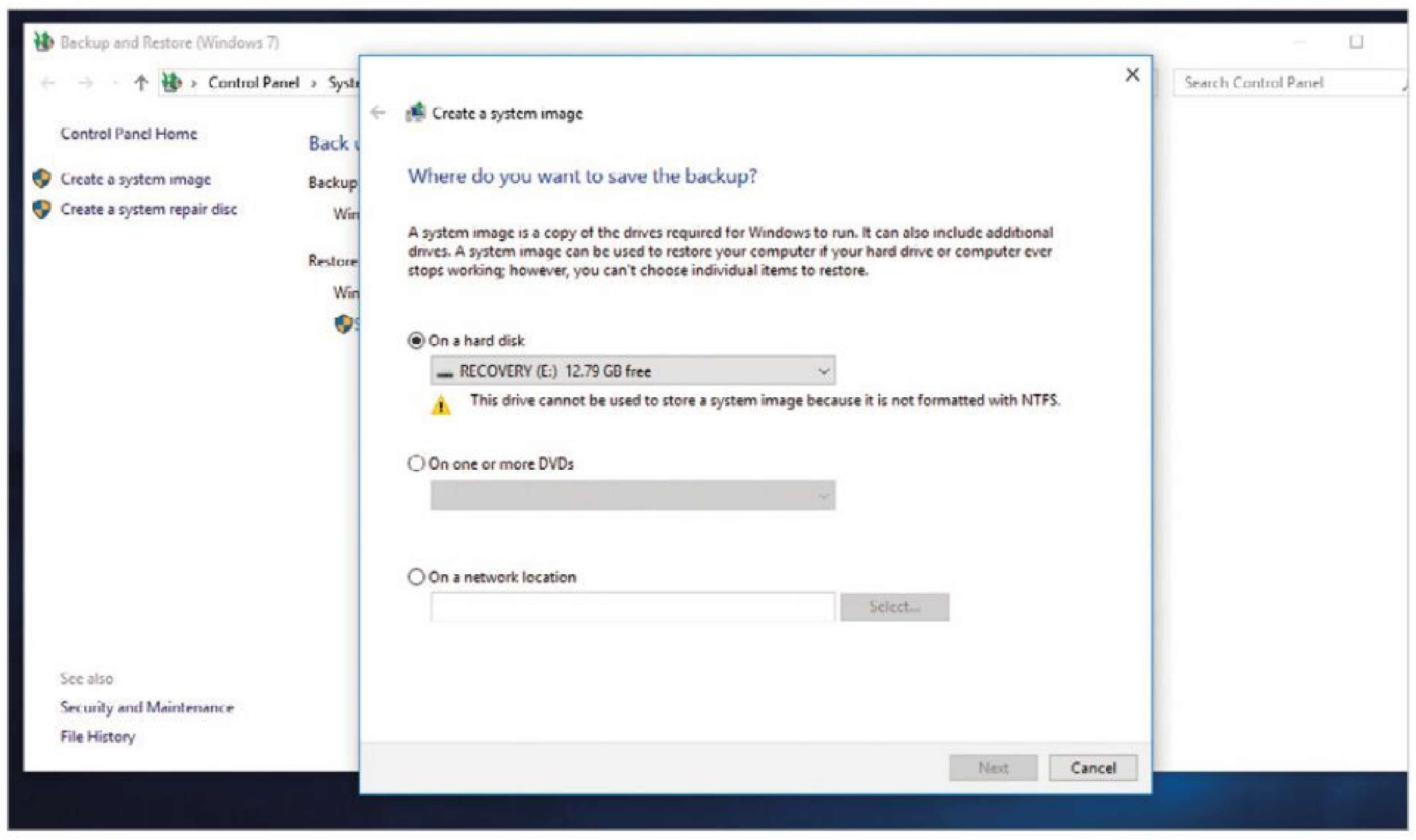
Backup

Windows Backup has not been set up.

Restore

Windows could not find a backup for this computer.

STEP 3 Windows will now scan your system for a drive that is able to house the system image files. You may need to make some changes to any drives according to what messages you get back from the scan. In this example, the drive we're using needs to be formatted as NTFS before Windows 10 can use it.


Backup and Restore (Windows 7)
Control Panel
Search Control Panel
Control Panel Home
Create a system image
Create a system repair disc
See also
Security and Maintenance
File History
Next
Cancel
Select...

Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore.

● On a hard disk

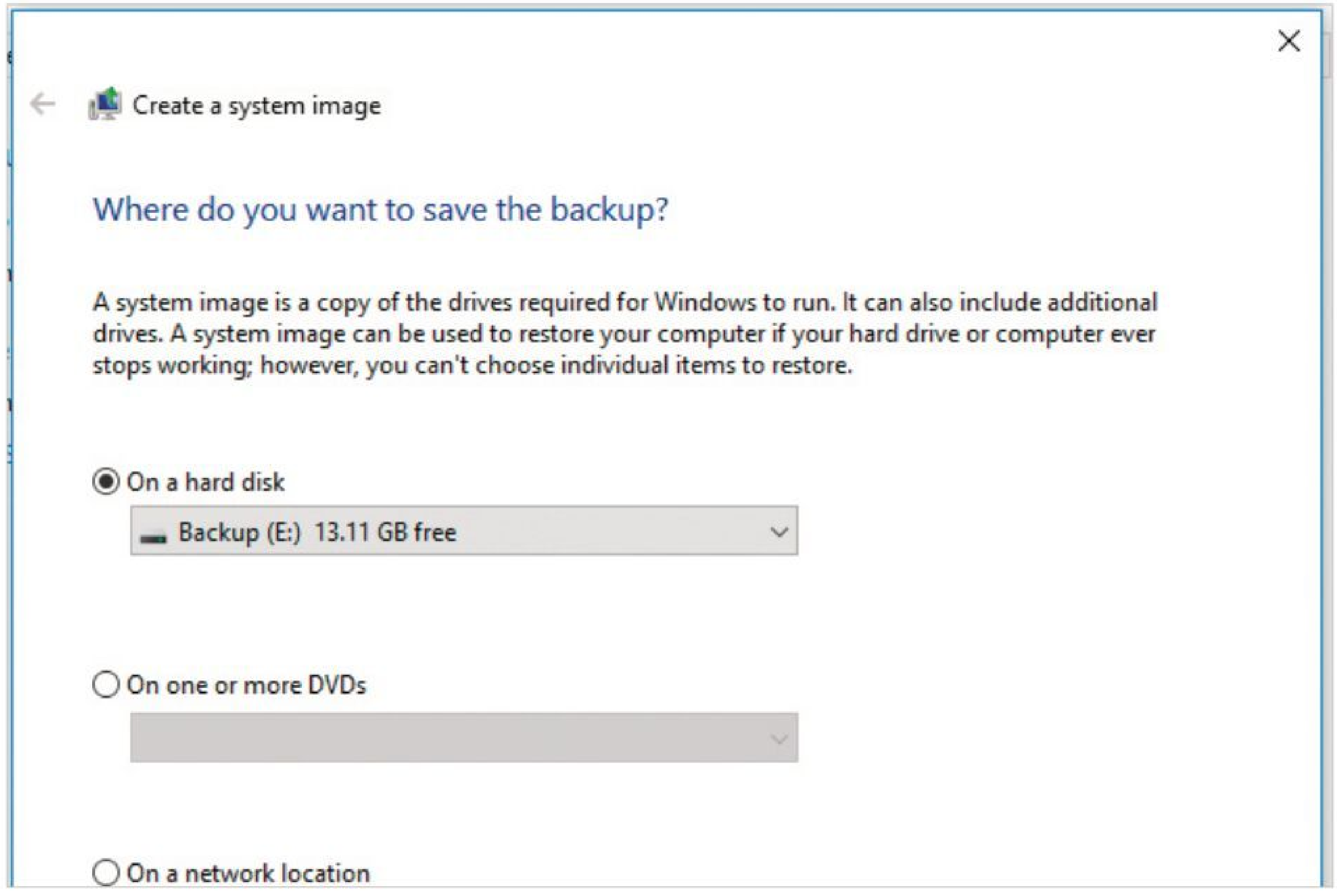
RECOVERY (E:) 12.79 GB free

This drive cannot be used to store a system image because it is not formatted with NTFS.

○ On one or more DVDs

○ On a network location

STEP 4 Providing you've met the requirements, you're offered a choice of where the system image can be written to. A drive is the quickest solution when it comes to restoring the image but you can opt for DVDs; it depends on the size of the image as to how many DVDs you need. You can even select a network location.



Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore.

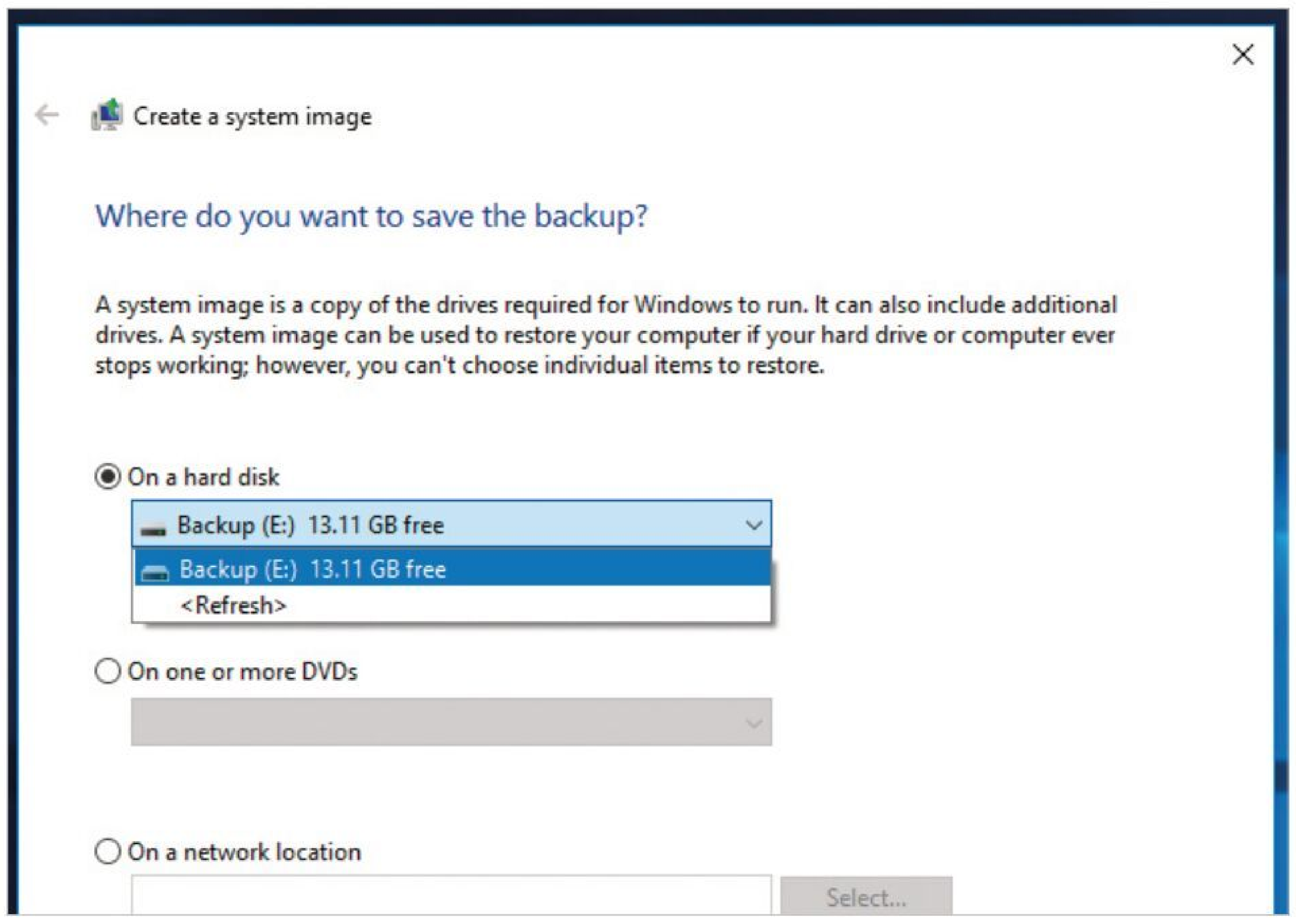
● On a hard disk

Backup (E:) 13.11 GB free

○ On one or more DVDs

○ On a network location

STEP 5 For this example, let's use an internal second hard drive. Make sure that the correct drive (it could be a high capacity USB stick or even portable USB hard drive) is selected, then click the Next button to continue.


Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore.

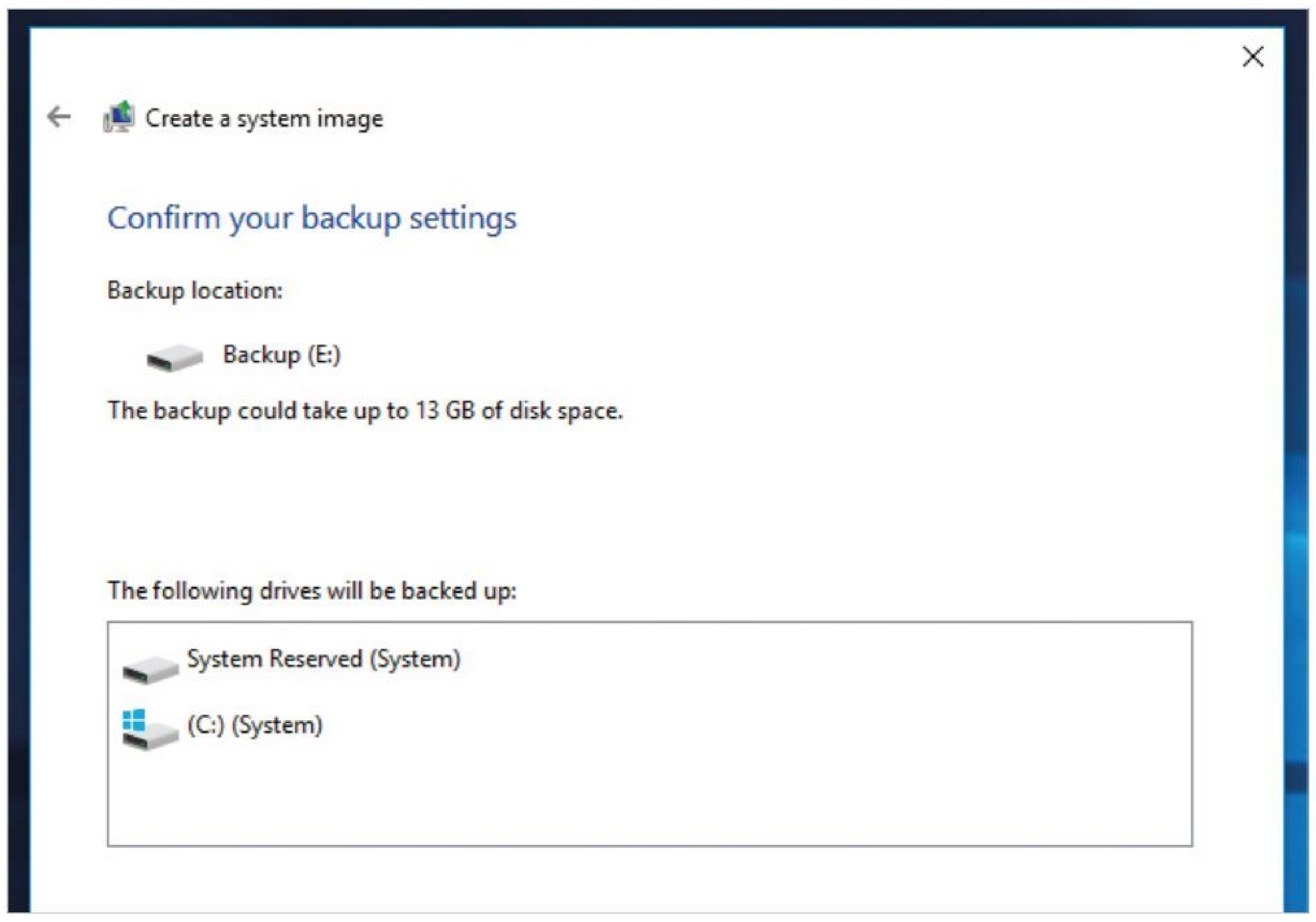
● On a hard disk

Backup (E:) 13.11 GB free

○ On one or more DVDs

○ On a network location

STEP 6 The next window will display the drives that are included in the system imaging process. In this example, the C:\ drive, the system drive and the System Reserved partition are to be backed up. When it comes to restoring the system you'll need both partitions for Windows 10 to be able to boot up correctly.


Create a system image

Confirm your backup settings

Backup location:

Backup (E:)

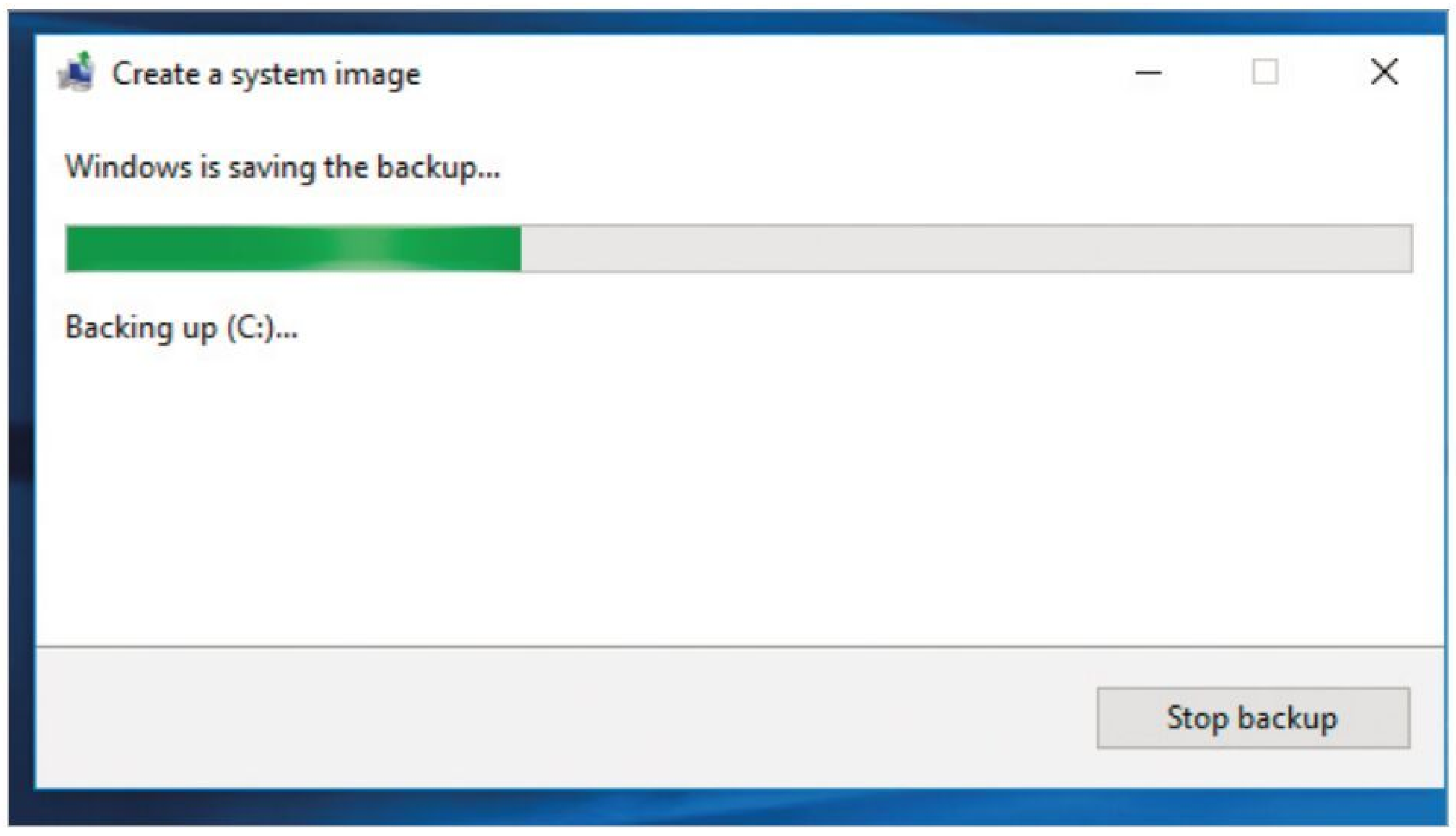
The backup could take up to 13 GB of disk space.

The following drives will be backed up:

System Reserved (System)

(C:) (System)

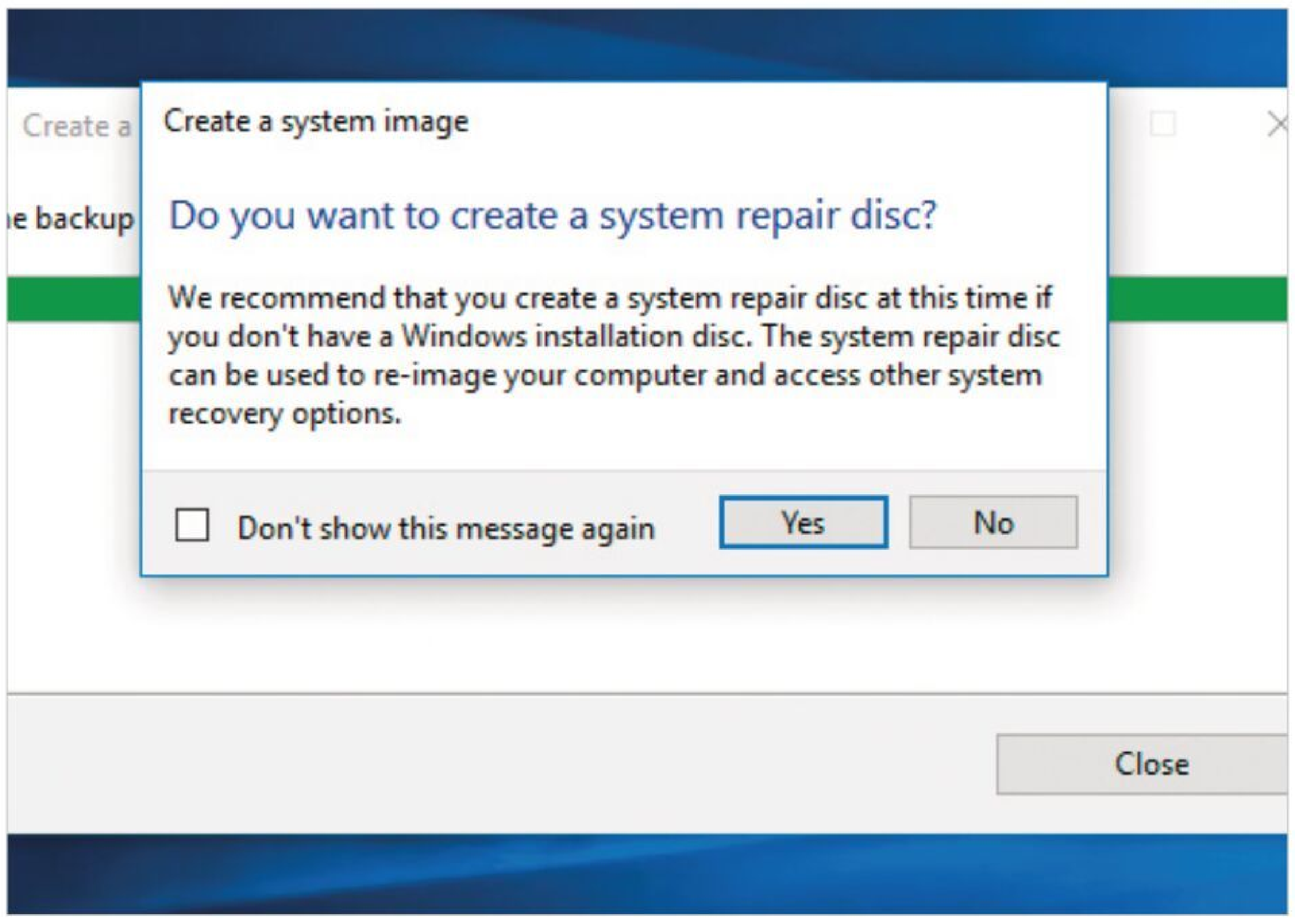
STEP 7 When you're ready to continue, click the Start Backup button. This will begin the imaging process, which can take some time depending on the amount of space used on the C:\ drive and the speed of the drive you're writing to. Allocate ample time if you're writing to DVD.


Create a system image

Windows is saving the backup...

Backing up (C:)...

STEP 8 Once the process is complete, Windows will ask you to create a System Repair Disc. This disc will allow you to boot into the environment where you are able to launch the system image restore.

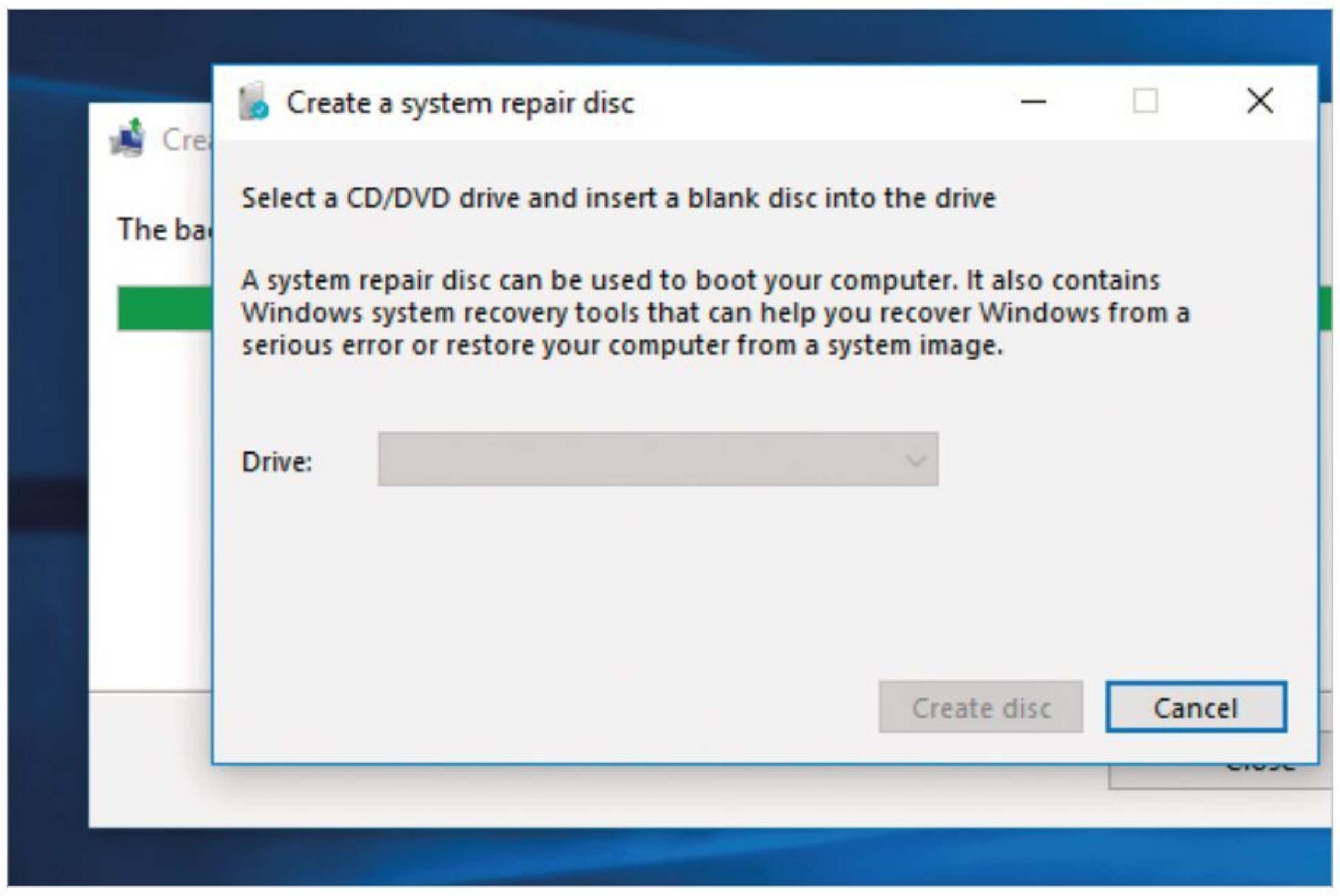

Create a system image

Do you want to create a system repair disc?

We recommend that you create a system repair disc at this time if you don't have a Windows installation disc. The system repair disc can be used to re-image your computer and access other system recovery options.

☐ Don't show this message again

STEP 9 If you click Yes to creating the System Repair Disc you need to make sure you have a blank DVD to hand. Follow the on-screen instructions and click on the Create Disc button to burn the repair files to the disc.

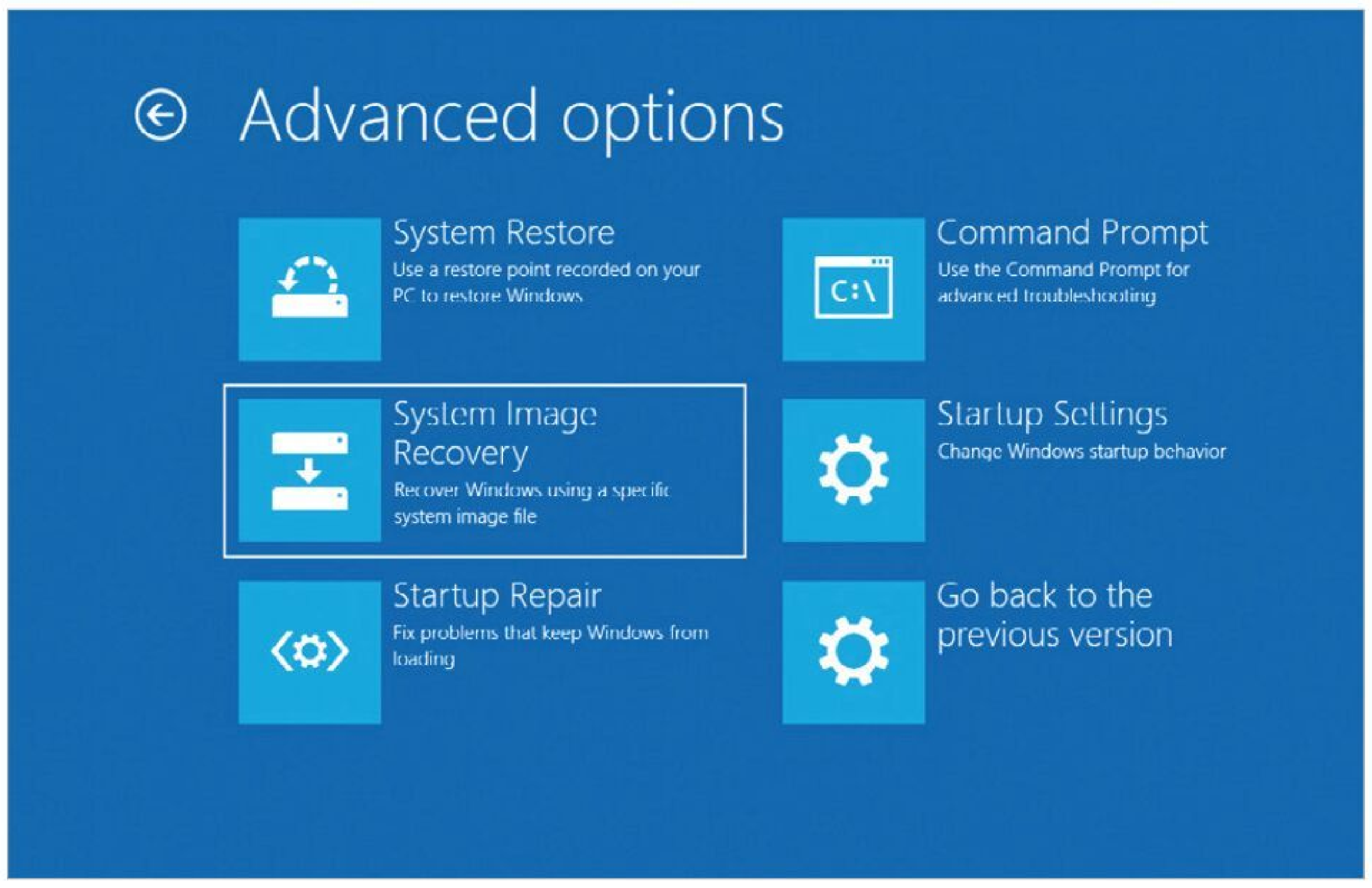

Create a system repair disc

Select a CD/DVD drive and insert a blank disc into the drive

A system repair disc can be used to boot your computer. It also contains Windows system recovery tools that can help you recover Windows from a serious error or restore your computer from a system image.

Drive:

STEP 10 Should you need to restore Windows 10 from the system image, you can boot into the System Repair Disc and select the System Image Recovery option from within the Advanced Options of the Trouble Shoot menu. Follow the instructions and within minutes Windows 10 will be back as it was when the system image was taken.


Advanced options

System Restore
Use a restore point recorded on your PC to restore Windows

Command Prompt
Use the Command Prompt for advanced troubleshooting

System Image Recovery
Recover Windows using a specific system image file

Startup Settings
Change Windows startup behavior

Startup Repair
Fix problems that keep Windows from loading

Go back to the previous version

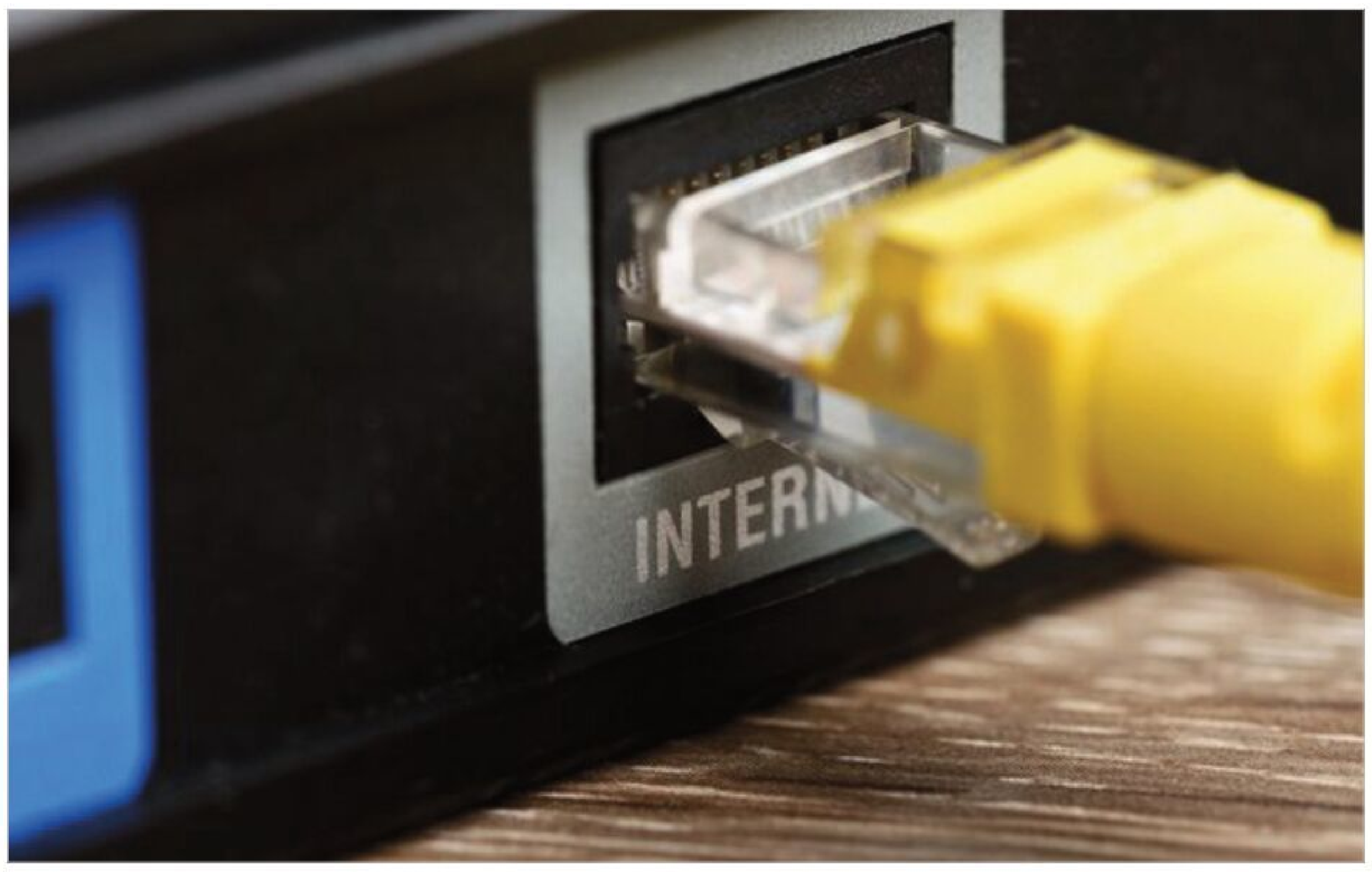
Extreme Windows 10 Lockdown Tips

There are numerous ways and means to greatly improve Windows 10's security and privacy. Precisely how secure and private you want to get is purely down to you. You can opt for better than average or through these tips below, absolute extreme security.

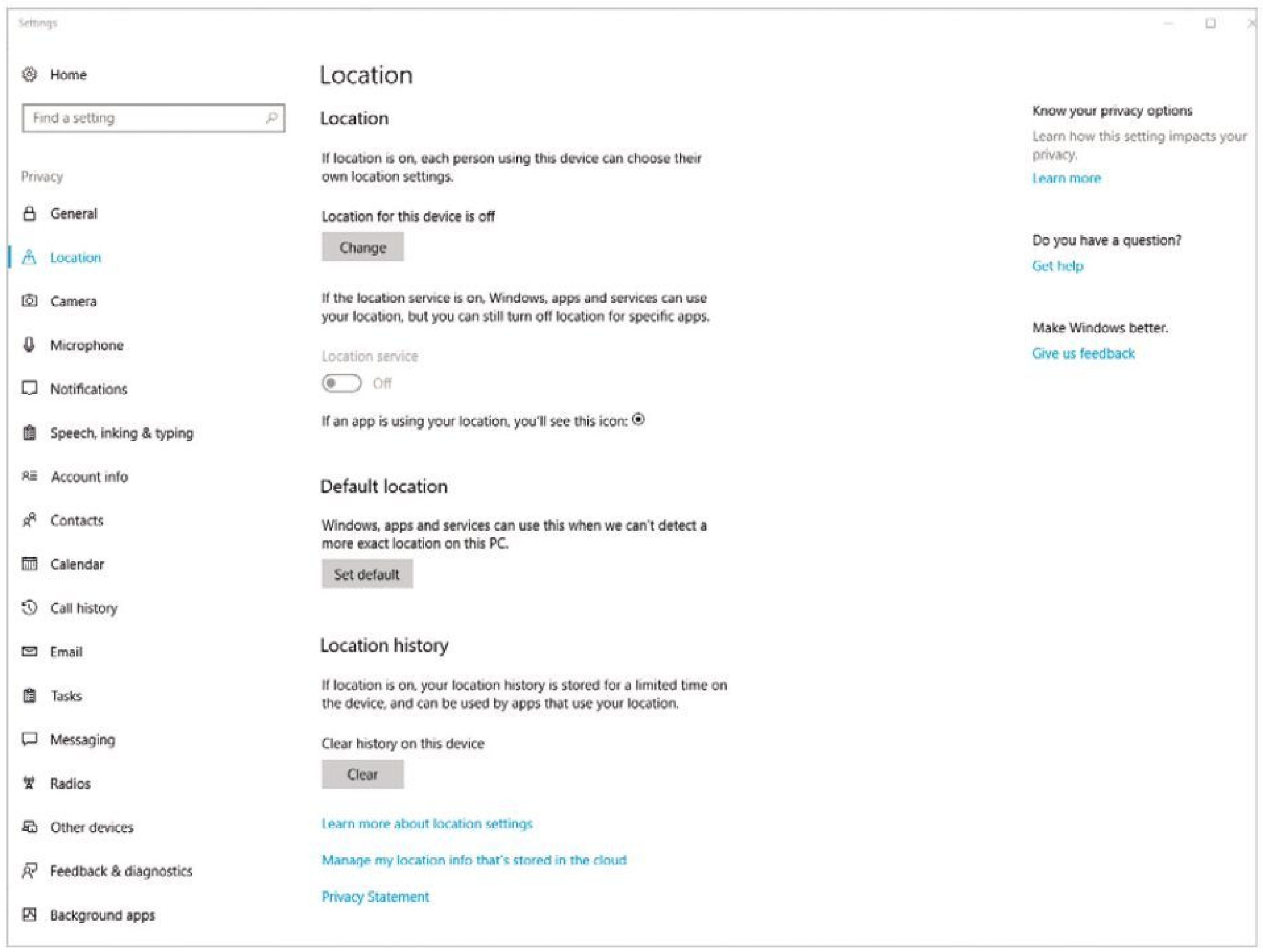
Windows 10 Security: The Paranoid's Guide

If you're fanatical about securing Windows 10 and locking it down to the point where the NSA would be impressed, then follow these top ten extreme lockdown tips.

TIP 1 Let's begin with the easiest tip, unplug the computer from the Internet. Naturally there are disadvantages to this and you won't get updates for Windows or programs. However, you certainly won't get any Internet-borne malware infecting your machine.



TIP 2 Click the Windows Start button and type privacy into the search box. Open the Privacy Settings link and turn off every option within the eighteen available Privacy sub-categories to the left of the console window.


Settings
Home
Find a setting
Privacy
General
Location
Camera
Microphone
Notifications
Speech, inking & typing
Account info
Contacts
Calendar
Call history
Email
Tasks
Messaging
Radios
Other devices
Feedback & diagnostics
Background apps
Change
Set default
Clear
Learn more
Get help
Give us feedback
Learn more about location settings
Manage my location info that's stored in the cloud
Privacy Statement

Location

Location

If location is on, each person using this device can choose their own location settings.

Location for this device is off

If the location service is on, Windows, apps and services can use your location, but you can still turn off location for specific apps.

Location service
Off

If an app is using your location, you'll see this icon: ◉

Default location

Windows, apps and services can use this when we can't detect a more exact location on this PC.

Location history

If location is on, your location history is stored for a limited time on the device, and can be used by apps that use your location.

Clear history on this device

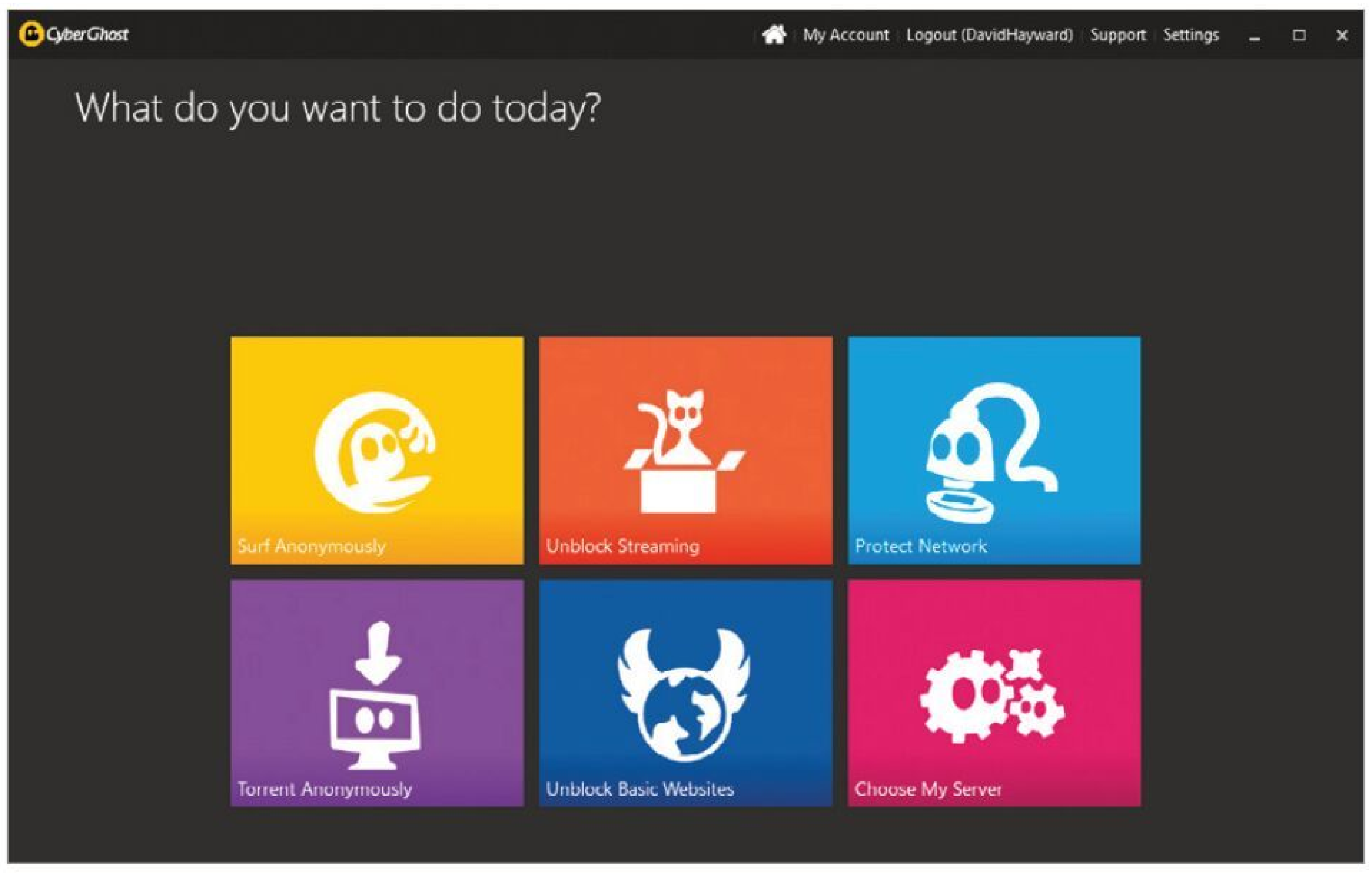
Know your privacy options

Learn how this setting impacts your privacy.

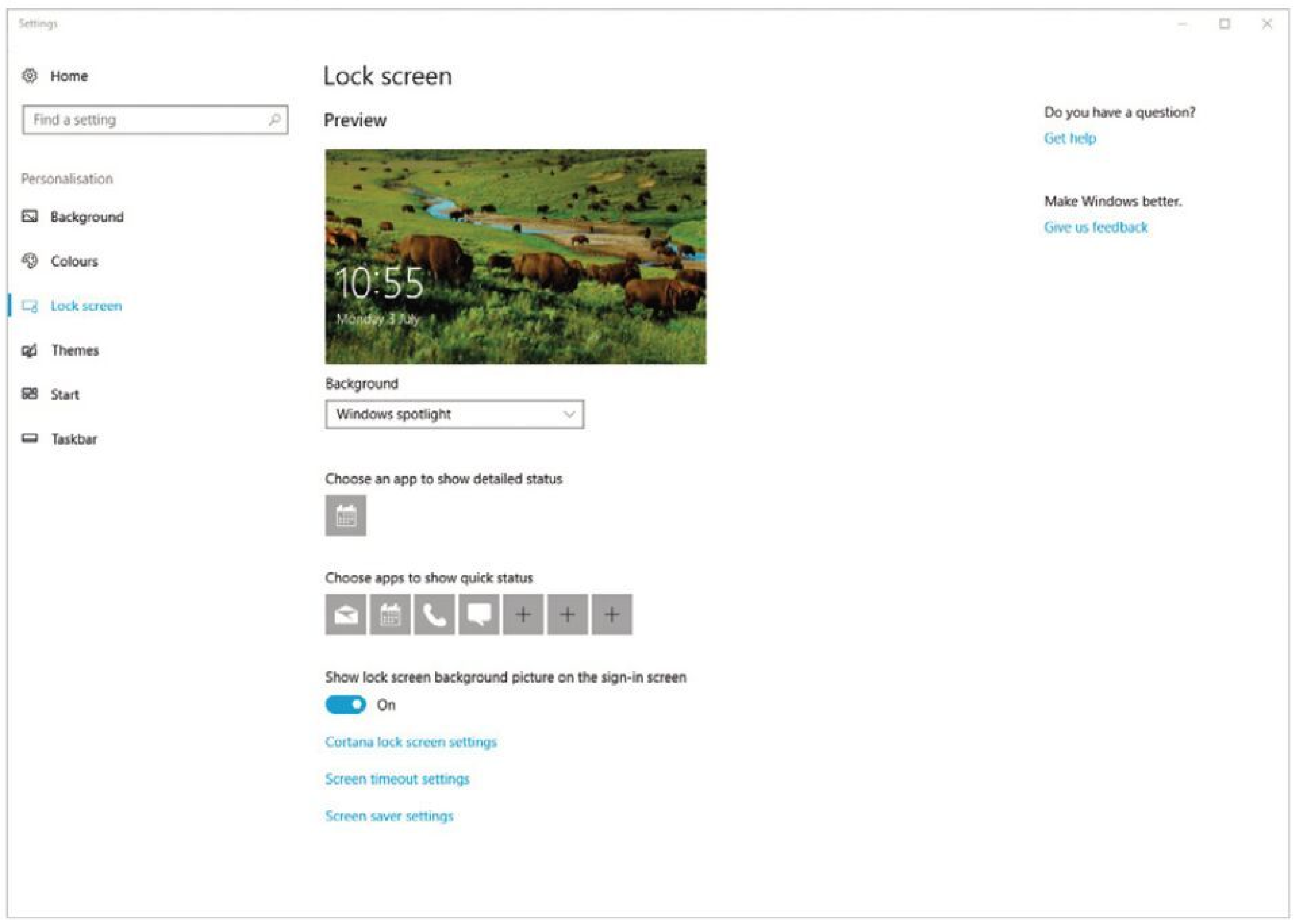
Do you have a question?

Make Windows better.

TIP 3 When online use a VPN and where possible, also use the Tor browser. Both of these combined will greatly improve your anonymity and improve security by utilising the site blocking and anti-scamming properties of a good VPN such as CyberGhost.


CyberGhost
My Account
Logout (DavidHayward)
Support
Settings
What do you want to do today?
Surf Anonymously
Unblock Streaming
Protect Network
Torrent Anonymously
Unblock Basic Websites
Choose My Server

TIP 4 If you step away from your computer on regular intervals, you need to make sure that no one will be able to get on to it. From the Windows Start button type lock and click the Lock Screen Settings link. In here set a lock so that only you can get back to your desktop once you've entered a password.


Settings
Home
Find a setting
Personalisation
Background
Colours
Lock screen
Themes
Start
Taskbar
10:55
Monday 3 July
Get help
Give us feedback
Cortana lock screen settings
Screen timeout settings
Screen saver settings

Lock screen

Preview

Background: Windows spotlight

Choose an app to show detailed status

Choose apps to show quick status

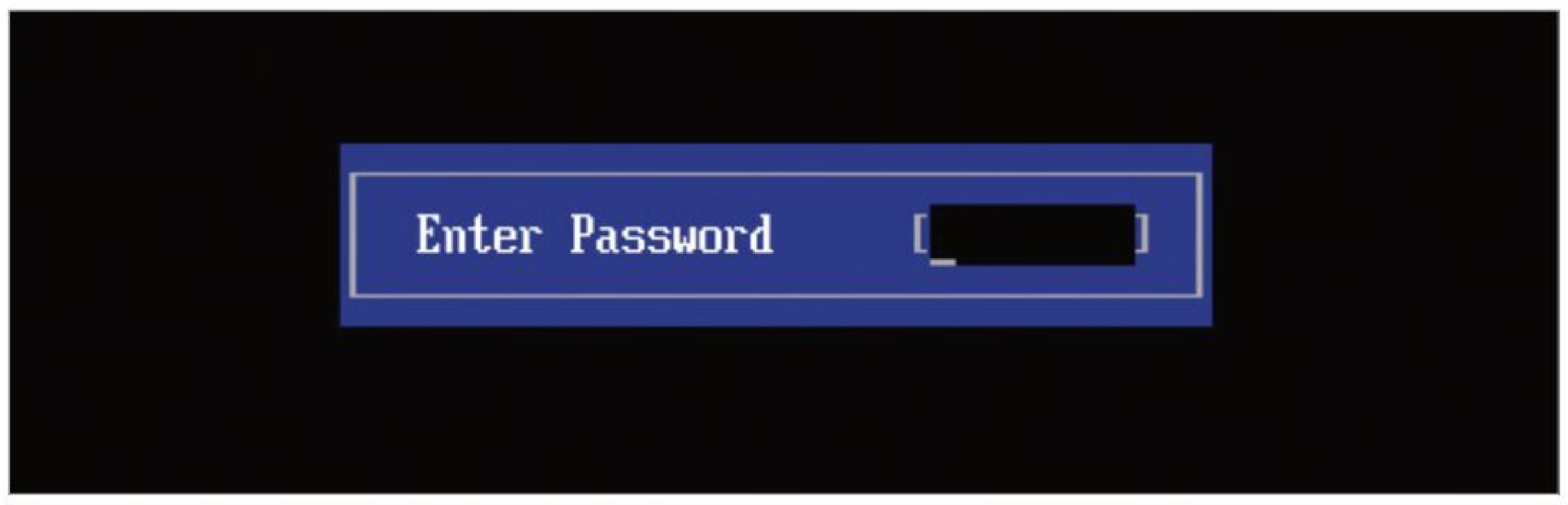
Show lock screen background picture on the sign-in screen
On

Do you have a question?

Make Windows better.

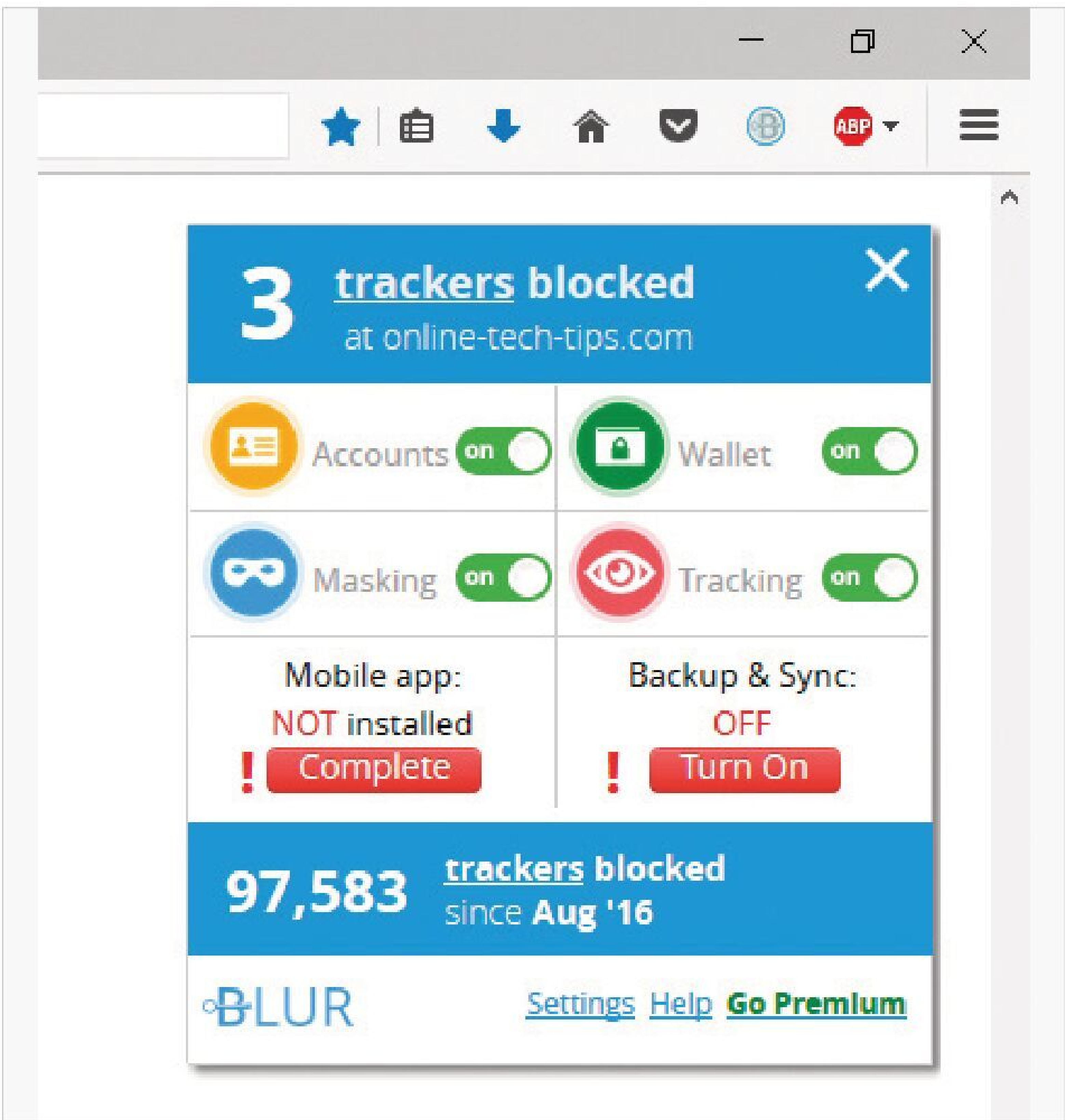
TIP 5

Depending on the age of your computer, it's possible to create a boot password from the BIOS. You need to consult your motherboard manual as to how to accomplish this but you can set a password for being able to boot into your computer (before Windows even starts) and getting into the BIOS itself.


Enter Password [ ]

TIP 6

Consider installing several add-ons to your browser to improve its security and prevent any unwanted data miners or rogue scripts from being executed. Adblock Plus, Blur, No Script and other examples will secure your browsing session. For an extreme route, use the Tor browser.


3 trackers blocked
at online-tech-tips.com

Accounts: on
Wallet: on
Masking: on
Tracking: on

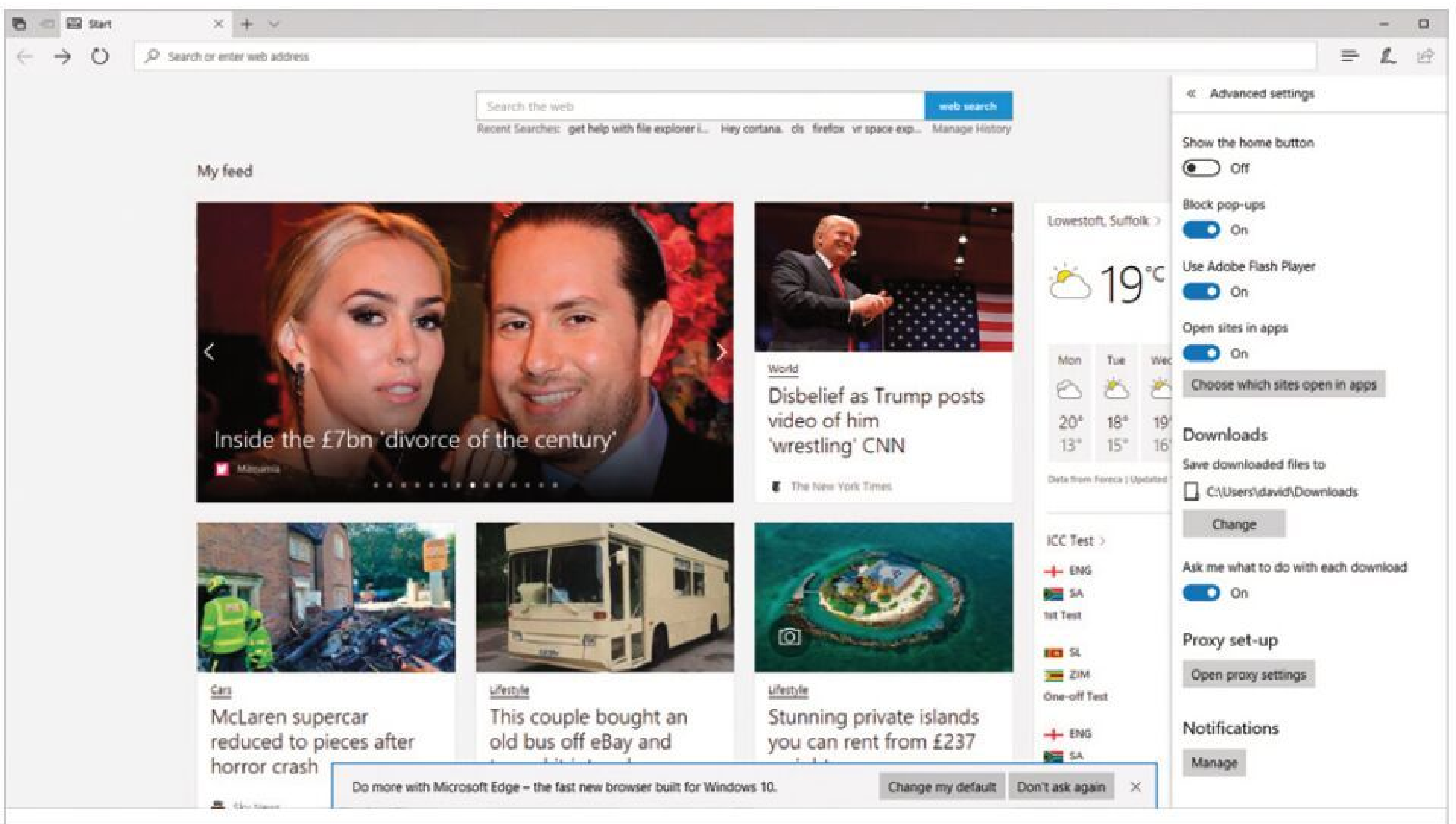
Mobile app: NOT installed
Backup & Sync: OFF

97,583 trackers blocked since Aug '16

ABP
Complete
Turn On
BLUR
Settings
Help
Go Premium

TIP 7

Flash and Java are superb entry points for malicious code to infect your computer and for snooping of various personal settings and data. Disabling both Java and Flash will prevent any such backdoors but limit your browsing experience on some sites.


Advanced settings

Show the home button: Off

Block pop-ups: On

Use Adobe Flash Player: On

Open sites in apps: On

Downloads

Save downloaded files to: C:\Users\david\Downloads

Ask me what to do with each download: On

Proxy set-up

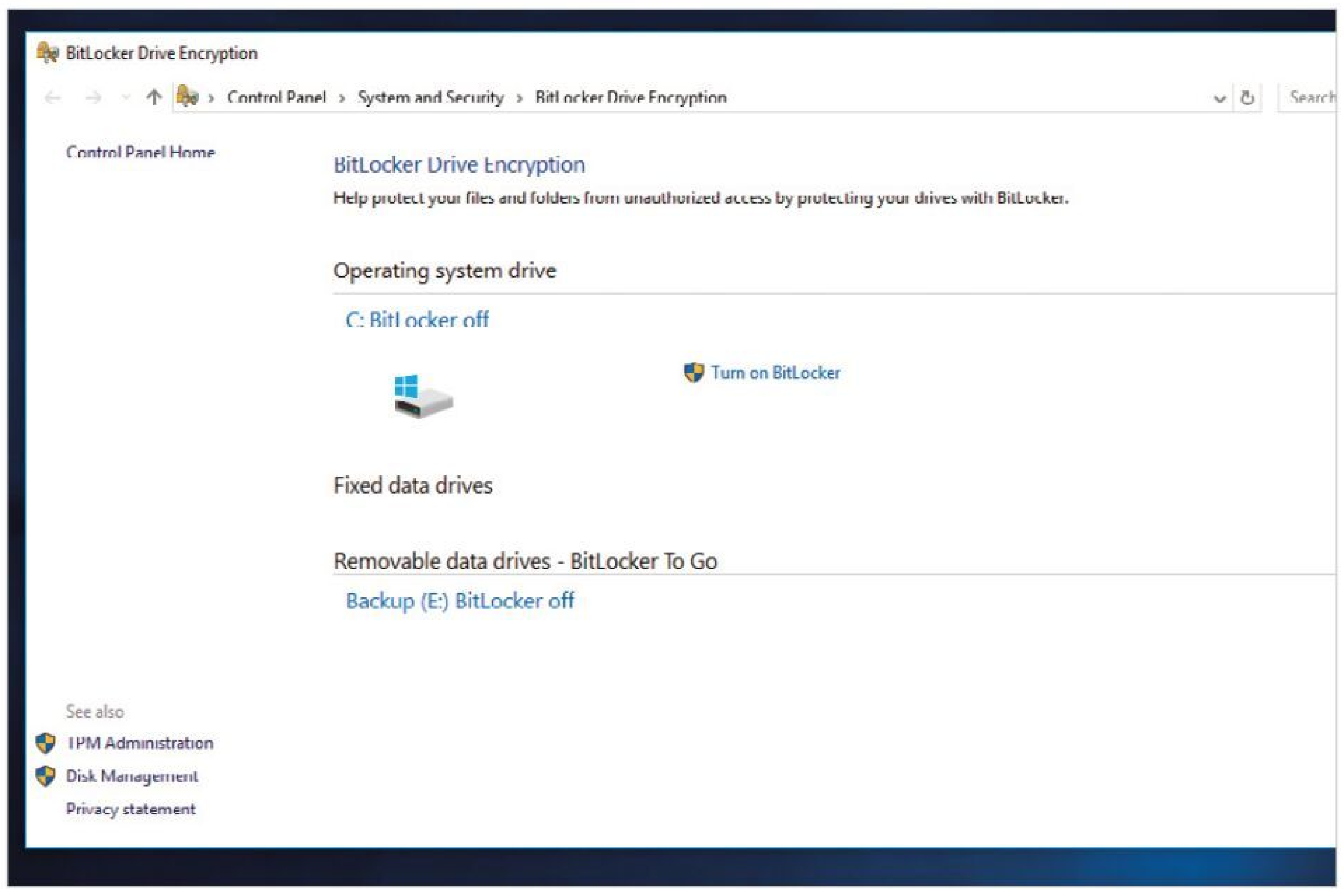
Notifications

Do more with Microsoft Edge – the fast new browser built for Windows 10.

Start
Search or enter web address
Search the web
web search
My feed
Inside the £7bn 'divorce of the century'
Disbelief as Trump posts video of him 'wrestling' CNN
The New York Times
Lowestoft, Suffolk
19°C
Mon
Tue
20° 13°
18° 15°
ICC Test
ENG
SA
SL
ZIM
One-off Test
McLaren supercar reduced to pieces after horror crash
This couple bought an old bus off eBay and
Stunning private islands you can rent from £237
Choose which sites open in apps
Change
Open proxy settings
Manage
Change my default
Don't ask again

TIP 8

Encrypting your installed hard drives and any external devices you use is an excellent way of securing your data and locking down Windows 10. Whilst it can be inconvenient, you can be safe in the knowledge that any lost data is virtually unhackable by all but the military supercomputers.


BitLocker Drive Encryption

Control Panel › System and Security › BitLocker Drive Encryption

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Fixed data drives

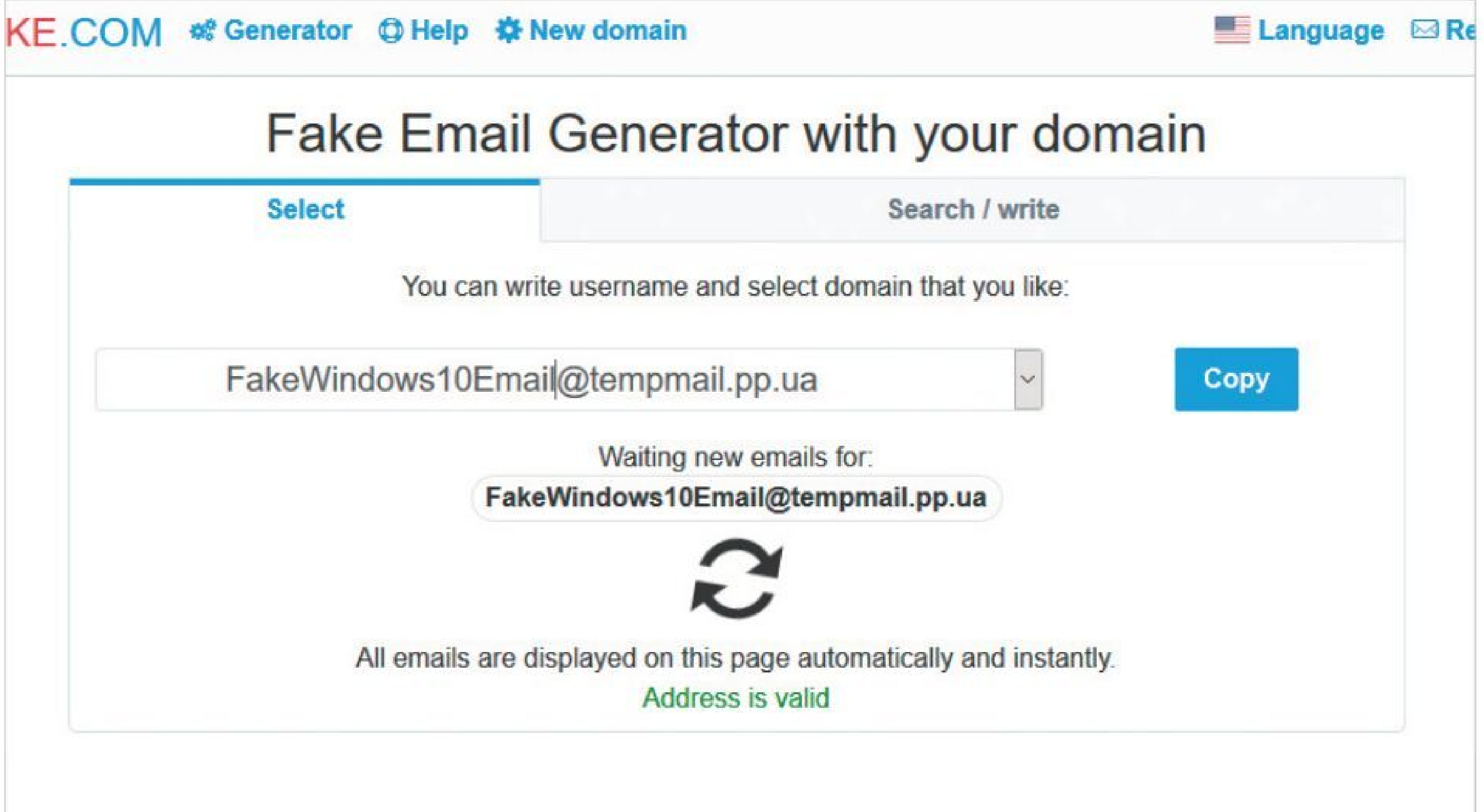
Removable data drives - BitLocker To Go

Backup (E:) BitLocker off

Control Panel Home
Search
Turn on BitLocker
See also
TPM Administration
Disk Management
Privacy statement

TIP 9

Normally you'd use a valid email account to log into Windows 10, via an activated Microsoft account. However, consider setting up an alternative account that isn't linked to you. That way any data sent via Windows 10 to other sources won't contain any personal data.


Fake Email Generator with your domain

You can write username and select domain that you like:

FakeWindows10Email@tempmail.pp.ua

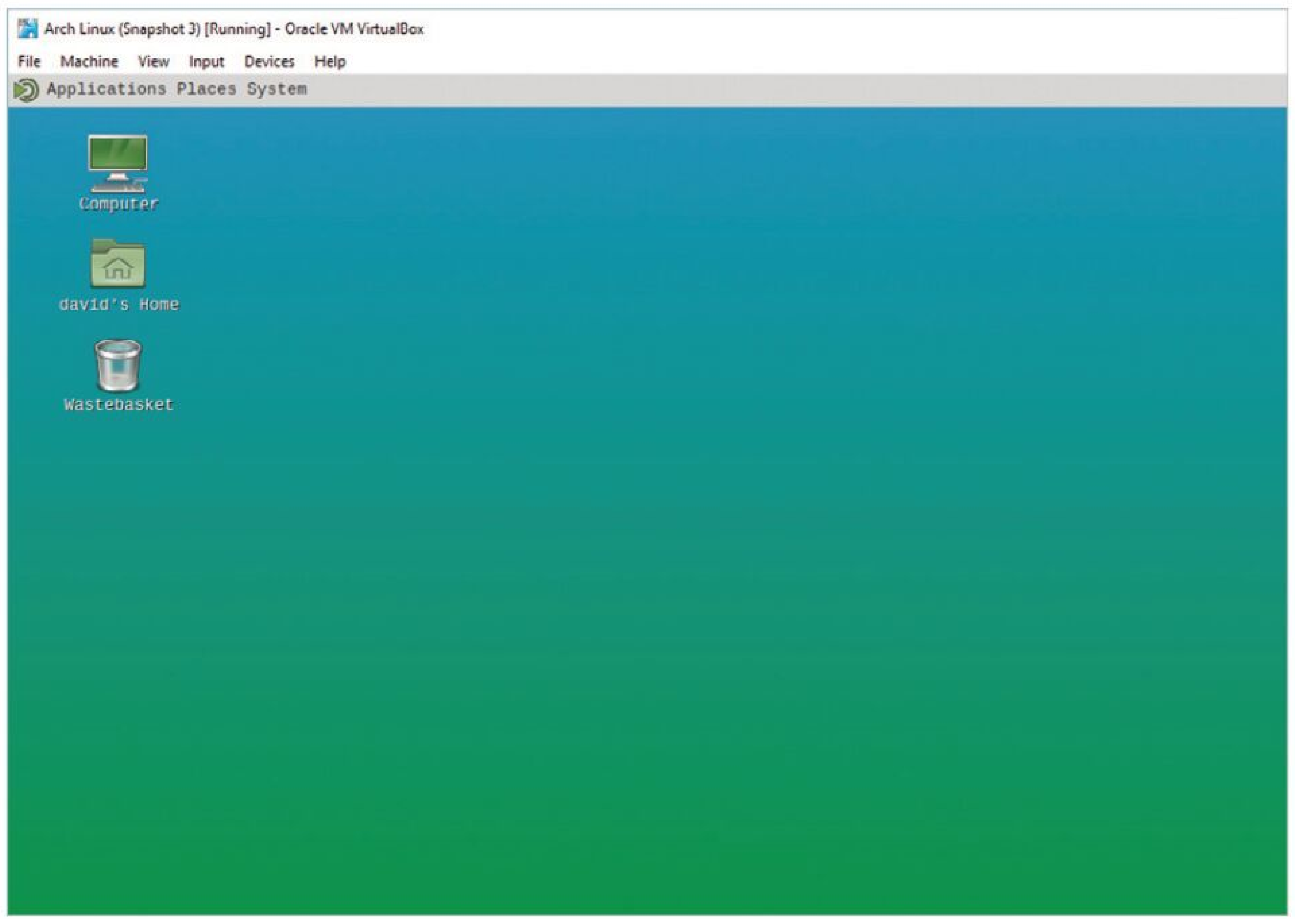
Waiting new emails for:
FakeWindows10Email@tempmail.pp.ua

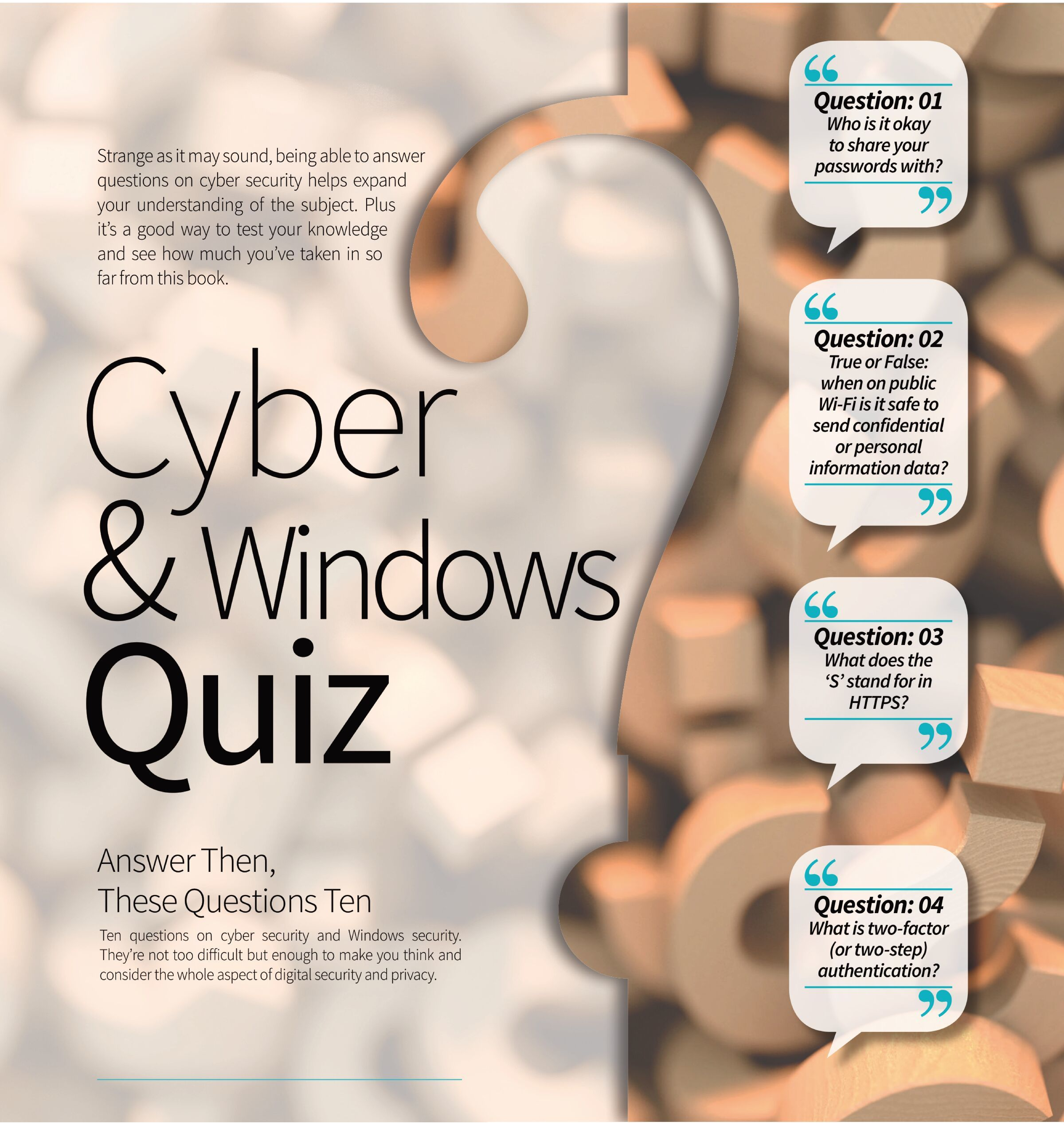
All emails are displayed on this page automatically and instantly.
Address is valid

KE.COM
Generator
Help
New domain
Language
Re
Select
Search / write
Copy

TIP 10

Use a Virtual Machine within Windows 10 to conduct your day to day browsing and online work. The VM could be Windows 10 too or even adopt a more secure environment such as one of the higher-end security versions of Linux. Either way, a VM will be far more secure than Windows 10 on its own.


Arch Linux (Snapshot 3) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Applications
Places
System
Computer
david's Home
Wastebasket



Strange as it may sound, being able to answer questions on cyber security helps expand your understanding of the subject. Plus it's a good way to test your knowledge and see how much you've taken in so far from this book.

Cyber & Windows Quiz

Answer Then, These Questions Ten

Ten questions on cyber security and Windows security. They're not too difficult but enough to make you think and consider the whole aspect of digital security and privacy.

Question: 01
Who is it okay to share your passwords with?

Question: 02
True or False: when on public Wi-Fi is it safe to send confidential or personal information data?

Question: 03
What does the 'S' stand for in HTTPS?

Question: 04
What is two-factor (or two-step) authentication?

Question: 05

Which of these is a Phishing attack?

- *Sending someone an email that contains a malicious link disguised as a valid email.*
- *Creating a fake website that looks identical to a real one, in order to trick users into logging in.*
- *Sending someone a text message that contains a malicious link, disguised as something else.*
- *All of the above.*

Question: 06

Which of the following passwords is the most secure?

- *Password123*
- *ThV%100*Vx!*
- *LetM31N*
- *123456*

Question: 07

Give five examples of malware

Question: 08

Which of these methods of browsing is the most secure?

- *HTTPS*
- *Private browser mode*
- *VPN*
- *Tor*

Question: 09

What does AES stand for?

Question: 10

How often should you review your Windows security and updates?

- *Once a month*
- *Once a day*
- *Once a week*
- *Once only, just after installation of Windows*

Answers:

1 *No one. Never tell anyone your passwords.*

2 *False. Never send personal or confidential data when using public Wi-Fi*

3 *Secure, meaning it's encrypted. Hyper Text Transfer Protocol Secure.*

4 *A multi-step authentication method requiring username and password, as well as extra information. Usually via a text message.*

5 *All of the above. All are forms of Phishing.*

6 *ThV%100*Vx!. It contains multiple characters, caps, lower case and isn't a dictionary word.*

7 *Ransomware, Virus, Adware, Trojan Horses, Worms.*

8 *VPN. Tor is very secure but is subject to vulnerabilities.*

9 *Advanced Encryption Standard.*

10 *Once a day. You should look at your Windows security at least once every day.*

What the Experts Say

Amongst the many quotes from security experts of the modern digital age, some stand out as either remarkably fortuitous or simply worth mentioning. We've compiled ten top quotes from the security world, that both entertain and make you think.

> “If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.”

White House Cybersecurity Advisor, Richard Clarke.

> “Computer security can simply be protecting your equipment and files from disgruntled employees, spies and anything that goes bump in the night, but there is much more. Computer security makes sure no damage is done to your data and that no one is able to read it unless you want them to.”

Bruce Schneier, Protect Your Macintosh, 1994.

> “Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds”

> “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.”

Gene Spafford.

> “No serious commentary will say that the user has no responsibility. We all have responsibilities to lock our doors in our homes and to buckle up when we get in cars.”

Spokesman, Information Technology Association of America, Business Roundtable, AP, May 19, 2004.

> “The condition of any backup is unknown until a restore is attempted.”

Schrodinger's Backup.

> “Phishing is a major problem because there really is no patch for human stupidity.”

Mike Danseglio, program manager in the Security Solutions group at Microsoft, April 4, 2006.

> “If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders.”

Dan Farmer, System Administrators Guide to Cracking.

> “The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it's easy to remember, it's something non-random like 'Susan'; and if it's random, like 'r7U2*Qnp,' then it's not easy to remember.”

Bruce Schneier.

> “Like the death of a celebrity from a drug overdose, publicised data loss incidents remind us that we should probably do something about taking better care of our data. But we usually don't, because we quickly remind ourselves that backups are boring as hell and that it's shark week on Discovery.”

Nik Cubrilovic, TechCrunch.com, October 10, 2008.

> “People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.”

Bruce Schneier, Secrets and Lies.

Online Child Protection

We as adults face numerous risks when online, children face significantly more. The predatory nature of some make the Internet an extremely hazardous place for a child to explore, despite the great benefits that it offers. The following pages will look at the risks involved for children when online but also how to prevent them and how to better protect your child while they navigate this virtual minefield.

Children Online: What are the Risks?

Every parent or guardian knows that being online represents an entirely new frontier of potential dangers for young children and teens. These dangers come in many forms, with each being capable of greatly affecting the lives of all involved.

The risks a child faces when online are tremendous and it's not just the usual collection of malware that focuses on luring young people into executing it. It's also the individuals, sites, language used, videos and a whole host of other forms of information and infiltration. These have quickly become the wolf in sheep's clothing, disguising themselves with the single purpose of catching hold of a child's online activities.

Grooming

One of the more prominent modes of luring children into saying or doing something they shouldn't is online grooming. The grooming itself could be for many different purposes, either to satisfy the perversions of an individual or group or to gain information on the family as a whole, and everything else in between.

Online grooming has evolved drastically in recent years with the expansion of social media. We'll look at the impact of social media and online grooming in the next couple of pages; suffice it to say however, that it's an on-going concern to parents and guardians, as well as those whose jobs involve the protection of young people.

Radicalisation

A more recent and newsworthy example of online dangers for children is radicalisation. This can come in the many different forms but essentially it's preying on young minds not yet capable of being able to discern between differing viewpoints in order to lure them into the mindset of those doing the radicalisation.

The more popular examples at present are extremist groups but it's not always something that's associated with terrorism or those groups affiliated with terrorist organisations. Radicalisation is the adoption of extreme political, social or religious ideals, ones that undermine contemporary ideas and the expressions of a nation. It's something that can occur quickly or over long periods of contact, with someone who follows this line of extremist thinking. Needless to say, it's something that a young mind can easily be tricked into believing and thus is something we as parents and guardians need to be aware of.

Inappropriate Content

The dangers of the Internet aren't always shady characters hanging around chat rooms pretending to be a twelve year old. Children with online access are just a stone's throw away from shocking, violent and pornographic material.

We've looked previously in this book at rogue links, or something masquerading as a valid website that can easily be used to send the hapless browser to a site that contains either something malicious or sinister, or simply something that's considered socially unacceptable.

Pornography sites are certainly of more prominent and easily accessible forms of unacceptable videos and images that children could venture into unsuspectingly. There are also many other forms of content that feature death, torture and other such despicable acts of violence. Either way, these are contents children should never witness.

Cyber Bullying

Cyber bullying comes from many diverse sources on the Internet. It's not simply others at school bullying someone on Facebook, Twitter etc., there are some startling statistics that detail the kind of bullying that occurs in online gaming.

For example, leading anti-bulling charity Ditch the Label, recently reported on a sample of 2,500 young people aged between 12 and 26. The report discovered that 64 percent were trolled whilst playing an online game; 57 percent experienced some form of bullying; half experienced hate speech and threats of violence; 39 percent received unwanted sexual contac;, 34 percent had private information shared; and 38 percent had been hacked whilst playing.

With comments such as 'I hope your parents die' and 'I'm coming to kill you', and children not being able to process this kind of violence, cyber bullying whilst playing online games is certainly an issue that needs addressing.

Identity Theft

Possibly used as part of grooming in order to gain information from a child, identity theft is a growing concern. Keeper Security, a leading password management app, recently published an infographic on web security. According to the company's sources, children are thirty five times more likely to have their identities stolen, with an estimated 1.3 million children affected each year by identity theft and nearly half of them under the age of six.

It's a shocking statistic and one that can lessened through online education and not leaving a child alone in front of the Internet; both not always easy to accomplish but also not impossible.

Online Scams

Children are vulnerable to varying forms of online scams purely due to their, in some ways, innocence and lack of experience, as well as acceptability of what they read to be a fact or truth. It's therefore quite easy to dupe a young person into a scam that either tries to take money from them, or some form of personal information.

The likely scams that children often fall for are usually related to gaming, i.e. 'click here to win 1000 in gold' 'get extra lives' or something that gives them an advantage in the latest game. Often scams will involve having them click a link that's offering to sell the latest games console, football kit, phones and other technology, all at unbelievably low prices. Naturally it's all fake but to a child it's an offer that's hard to refuse.

These are just some examples of what's out there and what lies in wait for a young person with an inquisitive mind and a trigger-happy mouse button. These individuals and groups have designed their risks to target children in particular, so we need to make doubly sure that when online our children are as educated, savvy and safe as possible.

> Whilst the Internet and all its contents are an incredible learning resource that can bring
>
> “
>
> ***Online Risks***
>
> ”
>
> together people from all over the world, inevitably there will be those who wish to exploit some of the most vulnerable among us, children and young people.

Social Media and Children

The impact of social media on children has been the subject of numerous reports over the last few years. With more and more children and young people gaining access to Facebook, Twitter, WhatsApp, Instagram and so on, there's a growing concern as to how it's affecting online safety.

Any site or portal where some form of social interaction occurs can be classed as social media, so even if you don't allow your children access to Facebook et al, there's still a chance they're in contact via gaming or an app of some description: YouTube, blogs and so on.

Reports from the American Academy of Paediatrics has found that using social media does provide benefits for young people. According to findings, regular use of social media platforms enhances communication, social connections and technical skills. Not only that, it allows young people to connect with extended family members and friends they won't see for perhaps years at a time, as they live in places they're not likely to visit. Depending on the content, social media can help a young person develop better perspectives on various issues in the media and when talked about with an adult, they can begin to form their own opinions, an impressive stage in a young person's life.

In some ways social media can help a young person express their inner feelings and encourages freedom of thought and engagement with similar age people. There's potential for a young person to learn new things, whether that's simple life hacks or discovering someone's job role. All in all, it adds up, on paper at least, to a positive experience that can greatly help a young person grow and help them form a more mature understanding of the world around them; something we didn't have before the Internet.

Sadly, with every positive aspect there are several negatives. Whilst the effects of social media on a child can be for good, they are mostly overshadowed by the popular negative aspects that ultimately rise to the surface. The sheer vastness of social media is one of the main causes for such negativity. Due to its freedom and limitless potential, there's no definable control on the scope of information. Yes, the social media platform can apply rules, filters and restrictions but these seem to be far too easily bypassed, and to some degree worthless in the end.

Cyber bullying is rife on social media. From threats made to young people, to digs at their appearance and body shaming, it's a platform that has quickly devolved into a pit of despair and depression for some unfortunate youngsters. This can lead, in extreme cases, to fatal consequences but generally the collective term for the negativity plied upon the youth of today is 'Facebook Depression'.

In recent months, the Royal Society for Public Health together with the Young Health Movement released a survey that revealed Instagram to have the negative impact on a young person's mental wellbeing, accusing the media platform of deepening young people's feelings of inadequacy and anxiety. It's a disturbing fact that on top of the pressures of school or college life, young people are having to put themselves through the mill whilst simply sitting in front of a screen.

Mental health is a major concern amongst young people but social media also presents its darker side through online grooming, potential radicalisation and the spread of malware. Each of these will greatly affect a young person and can lead to higher levels of anxiety, depression and withdrawal. For example, the spread of malware may not sound too negative on the wellbeing of a young person but put yourself in the place of the child who has unwittingly executed some form of malware on the family computer or the school network. The negative emotional effects from this happening can be huge to someone whose immaturity can't deal with the aftereffects.

The safety side of social media and children comes in many forms then. Mental health concerns, access to inappropriate content, Internet borne digital threats, bullying, grooming, loneliness and body image. Where it's easy to point out the risks of Internet stranger danger, it's not always easy to cover what happens should someone post edited and manipulated images of a young person to social media.

Therefore, the pressure on parents and guardians is just as immense, when helping our young people navigate the digital wild west frontier that is social media.

Using social media is amongst the most common online activities of the modern day young person. The likes of Facebook, Twitter, Instagram and many more all contribute to the billions of hours collectively spent via computers and mobile devices, with online gaming quickly following on the heels of the more popular social media portals.

> “***Safe Social Media***”

Search Engine Safety

The search engine is the portal into the wider Internet and through it we can view everything from man's first steps on the moon, to extremist group propaganda videos. It's therefore paramount that children are aware of the dangers of the search engine.

While the Google search portal isn't dangerous in itself, it's what potentially lies behind the search entered that makes it such a dangerous place for young people to venture into. Many young people are somewhat more tech-savvy than most adults but the younger children are at risk from a seemingly innocent search resulting in inappropriate content being displayed.

> **Safer Searching**

It doesn't take much imagination to consider how a particular scenario may be played out. A child is left in front of a search engine, they enter something to do with a school project on World War 2 and start to follow the links. Although part of history, some of the images that may be displayed could be deemed inappropriate to a primary school child, or those as young. To expand, what if the child then follows links to modern day warfare and from there potentially to videos depicting extreme violence. That then can snowball into accessing what can only be described as the real nasty stuff, which isn't something any child should ever witness.

The above scenario is, of course, the extreme end of what could potentially happen. Without going down the fearmongering road, the search engine can lead someone unsuspecting into a whole heap of trouble. That trouble can come from school, your ISP should any illegally hosted content be accessed, or even from accessing malware, so it's worth making sure that whatever search engine you use, any filters are currently set to On or Strict and it's recommended that you don't leave a child alone in front of a search engine for any length of time.

If you consider Google to be too risky, there are the likes of DuckDuckGo, a search engine that not only protects your data by not logging any searches but also features an extensive filter engine. Likewise StartPage, Bing, Boardreader and CC Search can also fulfil most users' requirements whilst filtering inappropriate content and allowing a higher degree of Internet privacy.

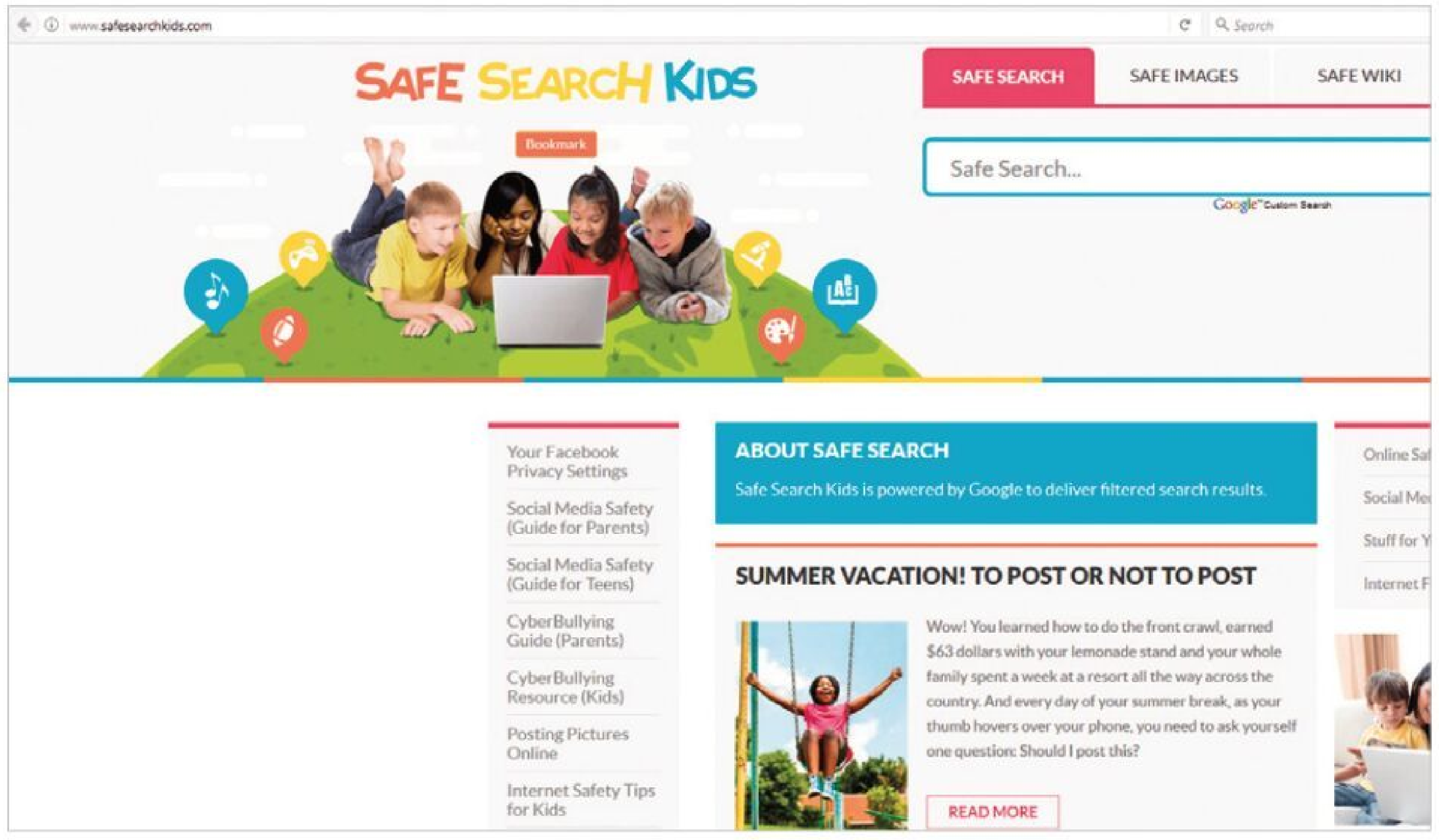
Alternatively there are steps we as parents, adults and guardians can do to help prevent any inappropriate content from appearing in a search result. There are numerous sites that have been designed specifically for safer searching with children in mind. The strict search policies of an engine may be good but there's always a chance that something could get through the net and reveal itself on the screen.

Six Safe Search Sites

Therefore, here are six child safe search engines. The age ranges vary but generally they're pitching to primary or low-middle school children. Either way, they're certainly worth considering and bookmarking for when a child is using the computer for school or general research.

SAFE SEARCH KIDS

A UK-based search engine that utilises Google's SafeSearch technology and provides a friendly front end. It's a good starting point and one that doesn't display picture icons along with search results; thus eliminating any inappropriate images that may unintentionally slip through.

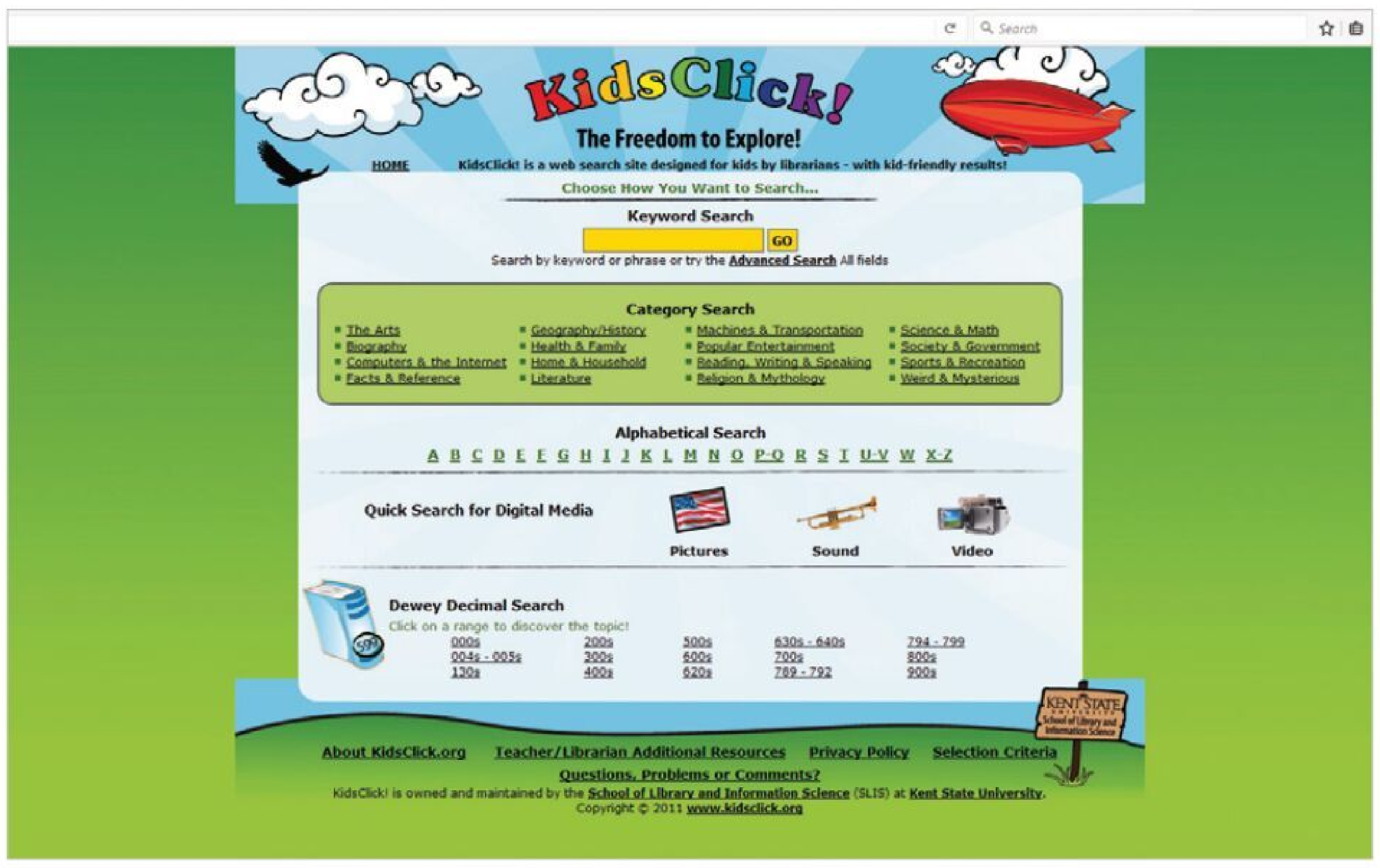


SAFE SEARCH KIDS
SAFE SEARCH
SAFE IMAGES
SAFE WIKI
Safe Search...
Bookmark
ABOUT SAFE SEARCH
SUMMER VACATION! TO POST OR NOT TO POST
READ MORE

Safe Search Kids is powered by Google to deliver filtered search results.

KIDSCLICK

KidsClick is a search engine designed and created by librarians for children who are searching for school related research. Each result returned features a description and reading level, along with suggestions and homework helpers.

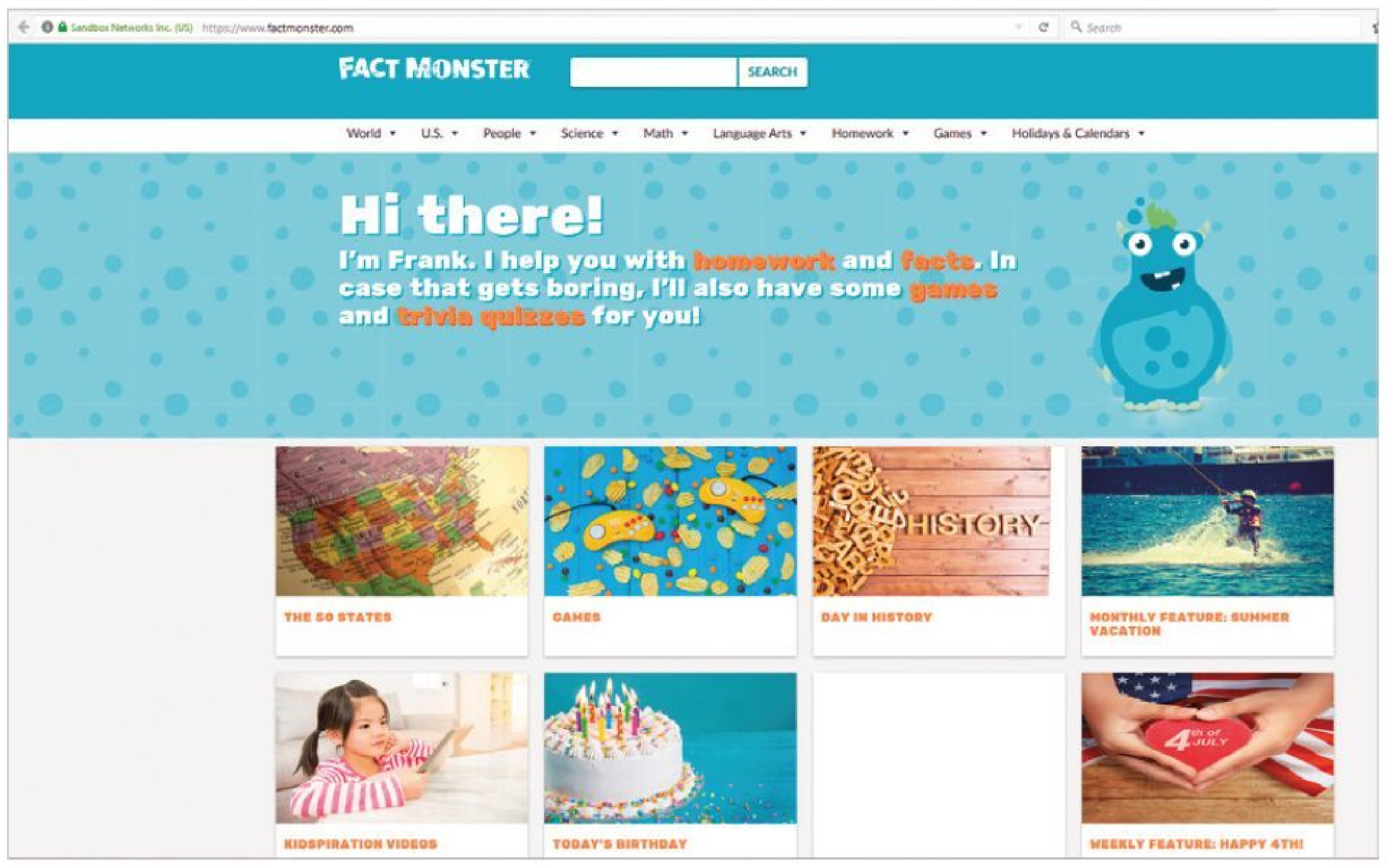


KidsClick!
The Freedom to Explore!
Keyword Search
GO
Category Search
Alphabetical Search
Quick Search for Digital Media
Pictures
Sound
Video
Dewey Decimal Search

KidsClick! is a web search site designed for kids by librarians - with kid-friendly results!

FACT MONSTER

Fact Monster is an excellent site that's dedicated to helping children research school topics. It's a free online almanac, dictionary, encyclopaedia and thesaurus and is aimed at children between the ages of eight and fourteen.

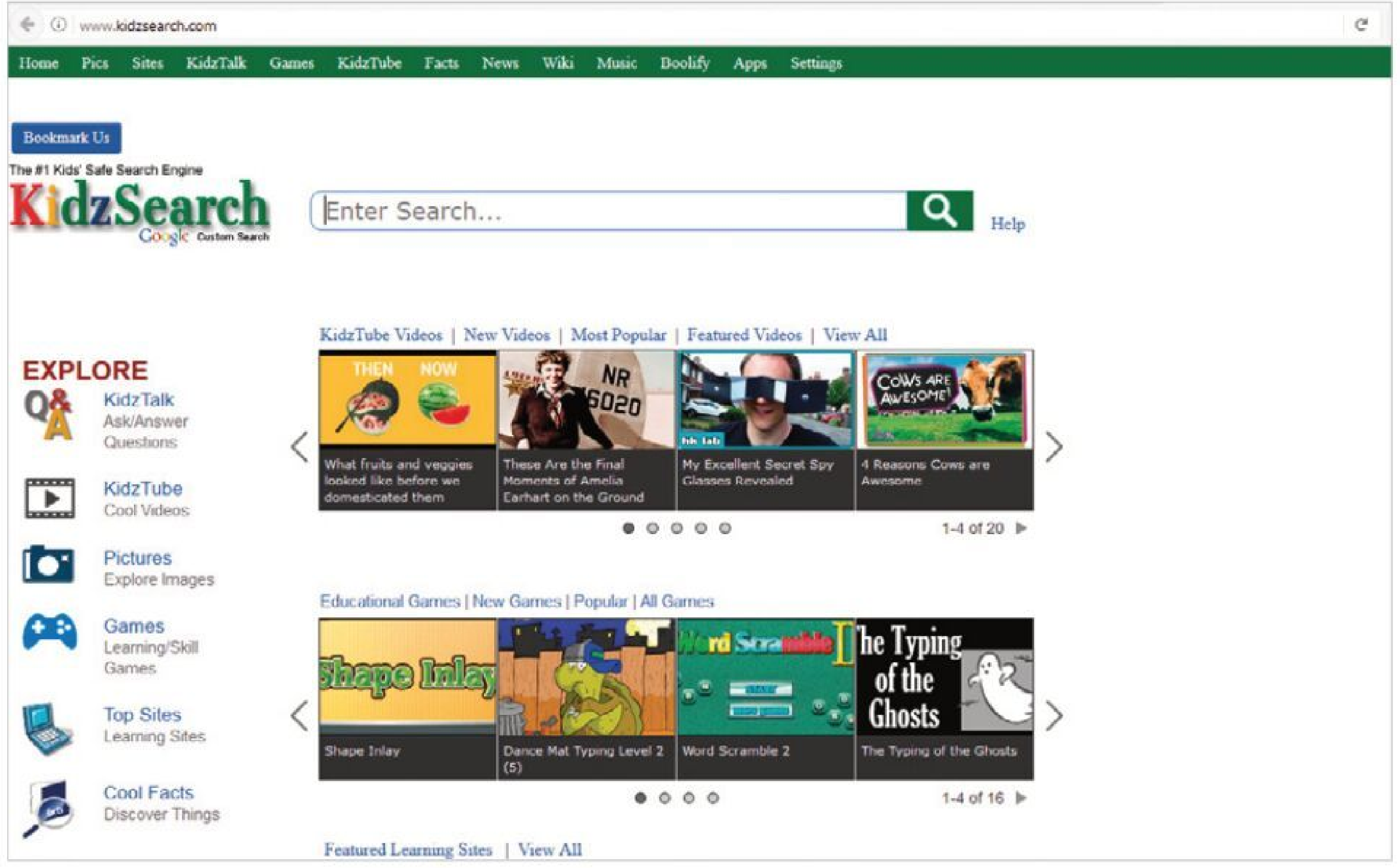


FACT MONSTER
SEARCH
World
U.S.
People
Science
Math
Language Arts
Homework
Games
Holidays & Calendars
THE 50 STATES
GAMES
DAY IN HISTORY
MONTHLY FEATURE: SUMMER VACATION
KIDSPIRATION VIDEOS
TODAY'S BIRTHDAY
WEEKLY FEATURE: HAPPY 4TH!

Hi there! I'm Frank. I help you with homework and facts. In case that gets boring, I'll also have some games and trivia quizzes for you!

KIDZSEARCH

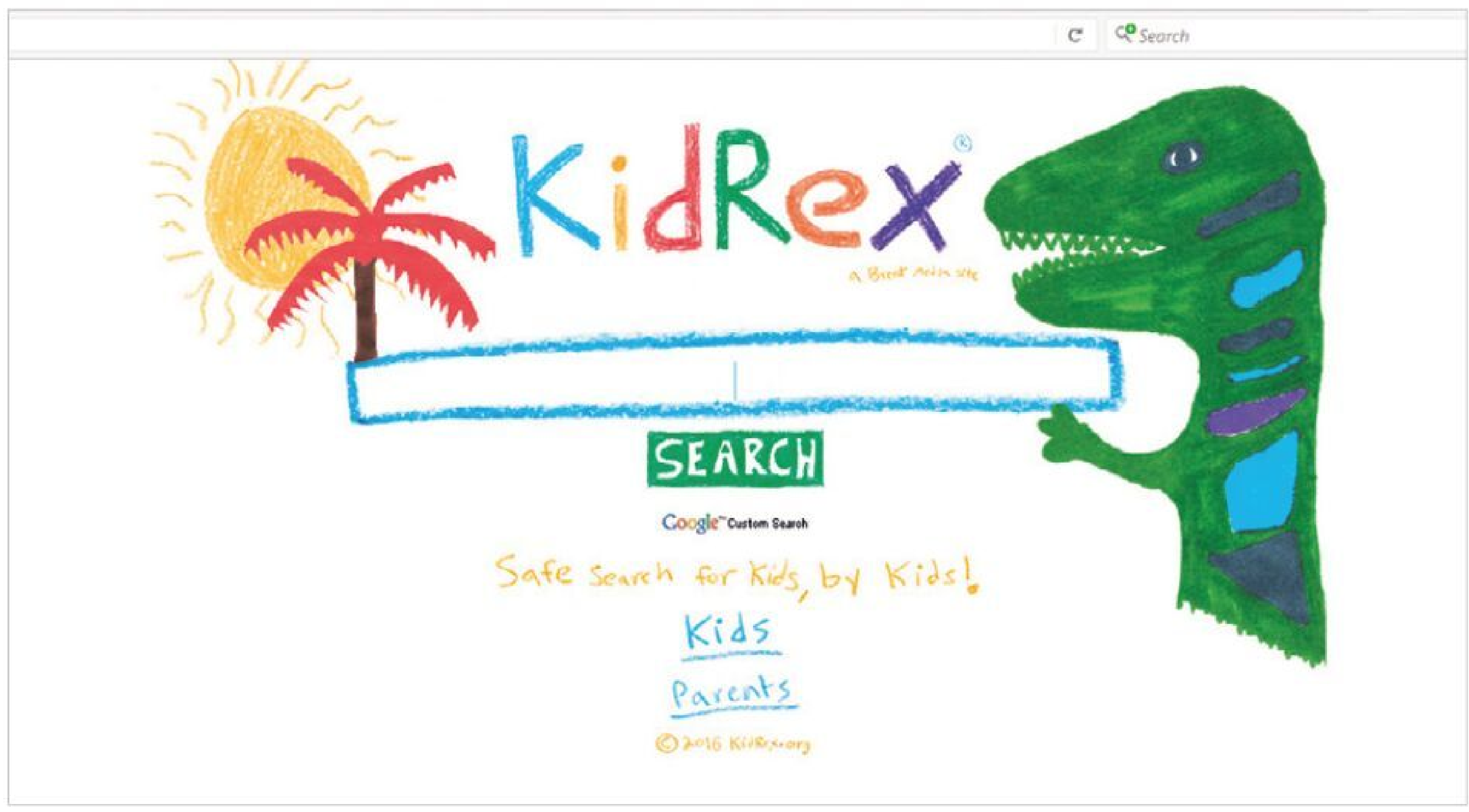
Here's another customised search engine utilising Google's SafeSearch strict results filter. Additionally, it also features a banned keyword search system that will not return any results from the black list of banned words.



Home
Pics
Sites
KidzTalk
Games
KidzTube
Facts
News
Wiki
Music
Boolify
Apps
Settings
Bookmark Us
The #1 Kids' Safe Search Engine
KidzSearch
Enter Search...
Help
EXPLORE
KidzTalk
Ask/Answer Questions
KidzTube
Cool Videos
Pictures
Explore Images
Games
Learning/Skill Games
Top Sites
Learning Sites
Cool Facts
Discover Things
Shape Inlay
Word Scramble
The Typing of the Ghosts
Featured Learning Sites | View All

KIDREX

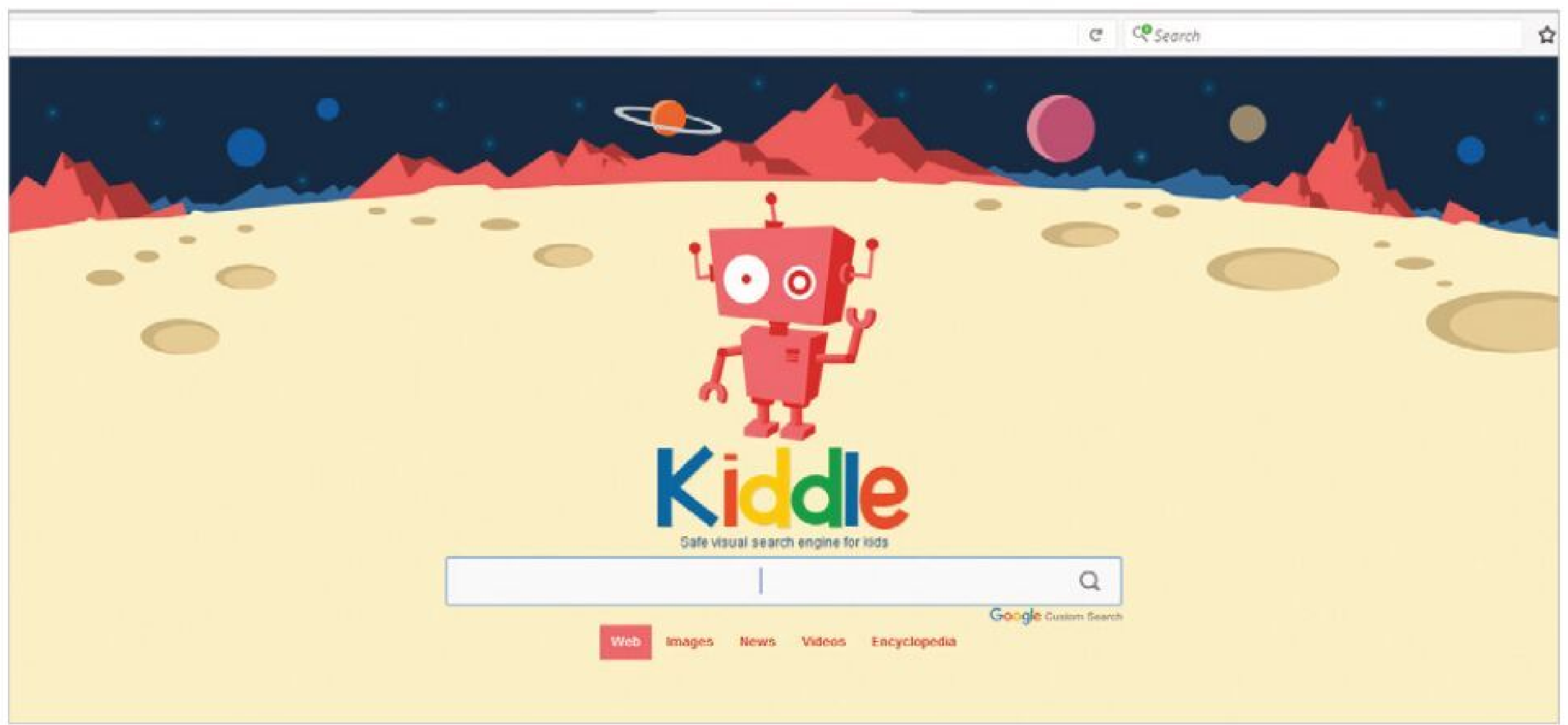
A simple site that's designed for much younger users. KidRex is powered by Google's own search engine but as you'd expect, filters out any inappropriate content. Further more, as a parent, you're also able to customise the filters to ensure safer or less restrictive search results.



KidRex
SEARCH
Google Custom Search
Safe Search for Kids, by Kids!
Kids
Parents

KIDDLE

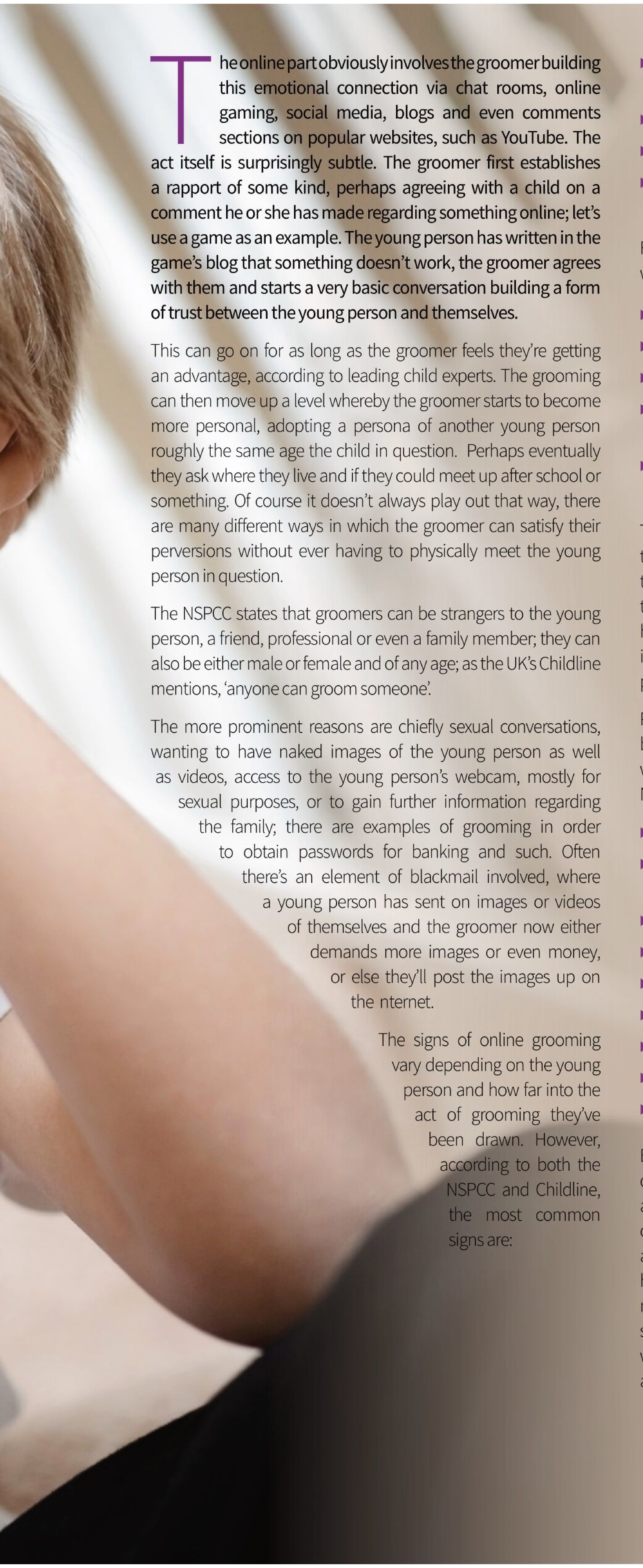
A great and friendly search engine for children and young people. Kiddle provides strict filtering along with child-friendly results that are grouped by those deemed safe and handpicked by the Kiddle editors. Here are trusted sites that aren't specifically written for children but provide understandable content and safe famous sites, that are harder to understand but still relevant.



Kiddle
Safe visual search engine for kids
Google Custom Search
Web
Images
News
Videos
Encyclopedia

Online Grooming

Of all the many despicable acts and threats that arise on the Internet toward young people, online grooming is undoubtedly one of the worst examples. It's a tricky act to confirm at times too, as those who groom often cleverly hide their tracks but it is possible to spot signs of it happening.



The online part obviously involves the groomer building this emotional connection via chat rooms, online gaming, social media, blogs and even comments sections on popular websites, such as YouTube. The act itself is surprisingly subtle. The groomer first establishes a rapport of some kind, perhaps agreeing with a child on a comment he or she has made regarding something online; let's use a game as an example. The young person has written in the game's blog that something doesn't work, the groomer agrees with them and starts a very basic conversation building a form of trust between the young person and themselves.

This can go on for as long as the groomer feels they're getting an advantage, according to leading child experts. The grooming can then move up a level whereby the groomer starts to become more personal, adopting a persona of another young person roughly the same age the child in question. Perhaps eventually they ask where they live and if they could meet up after school or something. Of course it doesn't always play out that way, there are many different ways in which the groomer can satisfy their perversions without ever having to physically meet the young person in question.

The NSPCC states that groomers can be strangers to the young person, a friend, professional or even a family member; they can also be either male or female and of any age; as the UK's Childline mentions, 'anyone can groom someone'.

The more prominent reasons are chiefly sexual conversations, wanting to have naked images of the young person as well as videos, access to the young person's webcam, mostly for sexual purposes, or to gain further information regarding the family; there are examples of grooming in order to obtain passwords for banking and such. Often there's an element of blackmail involved, where a young person has sent on images or videos of themselves and the groomer now either demands more images or even money, or else they'll post the images up on the nternet.

The signs of online grooming vary depending on the young person and how far into the act of grooming they've been drawn. However, according to both the NSPCC and Childline, the most common signs are:

- The young person being very secretive, including their online activity.
- Having older boyfriends or girlfriends.
- Going to unusual places to meet up with friends.
- Having new things such as clothes, phones or other objects they can't readily explain.

From the perspective of the young person, a groomer will usually:

- Send you lots of private messages.
- Ask you to keep conversations a secret.
- Attempt to find out more about you and your family.
- Start to send you sexual messages, usually starting with jokes then moving on.
- Blackmail you into sending images or videos by threats of violence to you or your family.

The situations can vary and the groomer is adept at hiding traces of their activity as well as lying to someone about themselves. Childline states: "It's important to remember that there isn't one type of groomer. Many different kinds of people have used the Internet to trick, force or persuade young people into sharing sexual images of themselves. Often it's an adult pretending to be a young person, but not always."

Parents and guardians can watch out for certain types of behaviour, which could be signs of grooming, regardless of whether it's online, via a phone chat app or even in person. The NSPCC have listed the following as potential signs:

- Withdrawn
- Suddenly behaves differently
- Anxious
- Clingy
- Depressed
- Aggressive
- Problems sleeping
- Eating disorders
- Wets the bed
- Soils clothes
- Takes risks
- Misses school
- Changes in eating habits
- Obsessive behaviour
- Nightmares
- Drugs
- Alcohol
- Self-harm
- Thoughts about suicide

Both Childline and the NSPCC have excellent websites dedicated to online grooming, along with advice to both parents and guardians, as well as young people and children. You can find them at https://childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-grooming/#10 and https://nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/grooming/. It's certainly worth reading through each site to gain a better understanding of online grooming, what the warning signs are and how to support a young person should any signs be apparent.

The NSPCC (the National Society for the Prevention of Cruelty to Children) defines grooming as when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking.

> **“*What it is and what to Look Out for*”**

How Safe are the Sites Your Child Can Access?

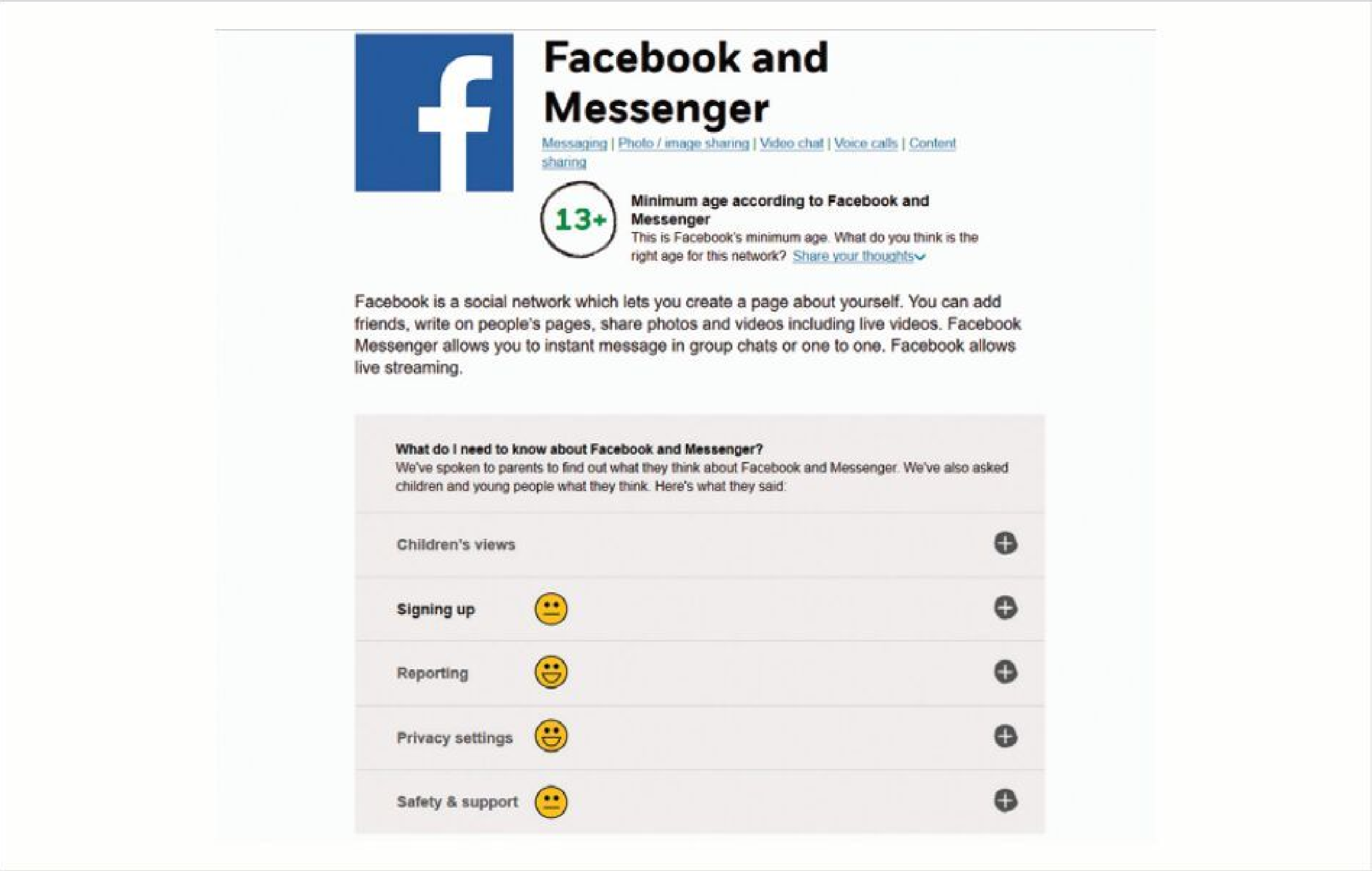
Mobile operator O2, YouGov and the NSPCC have teamed up with Net Aware to create a site that reviews popular sites and apps that children and young people use. This guide allows parents and guardians to view the information to help them understand their child's online world.

Net Aware

Net Aware is an excellent site, and can be found at https://net-aware.org.uk/. Within you can find an A to Z of Most Popular sites and how safe they actually are according to face icons. Here are ten of the popular choices with their safety information.

FACEBOOK AND MESSENGER

Facebook has gone to great lengths in recent years to ensure a higher degree of safety. There's a lot of ground left to cover but from the point of view of Net Aware, it's about average in terms of safety. Signing up and Safety & Support need looking into however.



Facebook and Messenger

Messaging | Photo / image sharing | Video chat | Voice calls | Content sharing

13+ **Minimum age according to Facebook and Messenger**
This is Facebook's minimum age. What do you think is the right age for this network? Share your thoughts

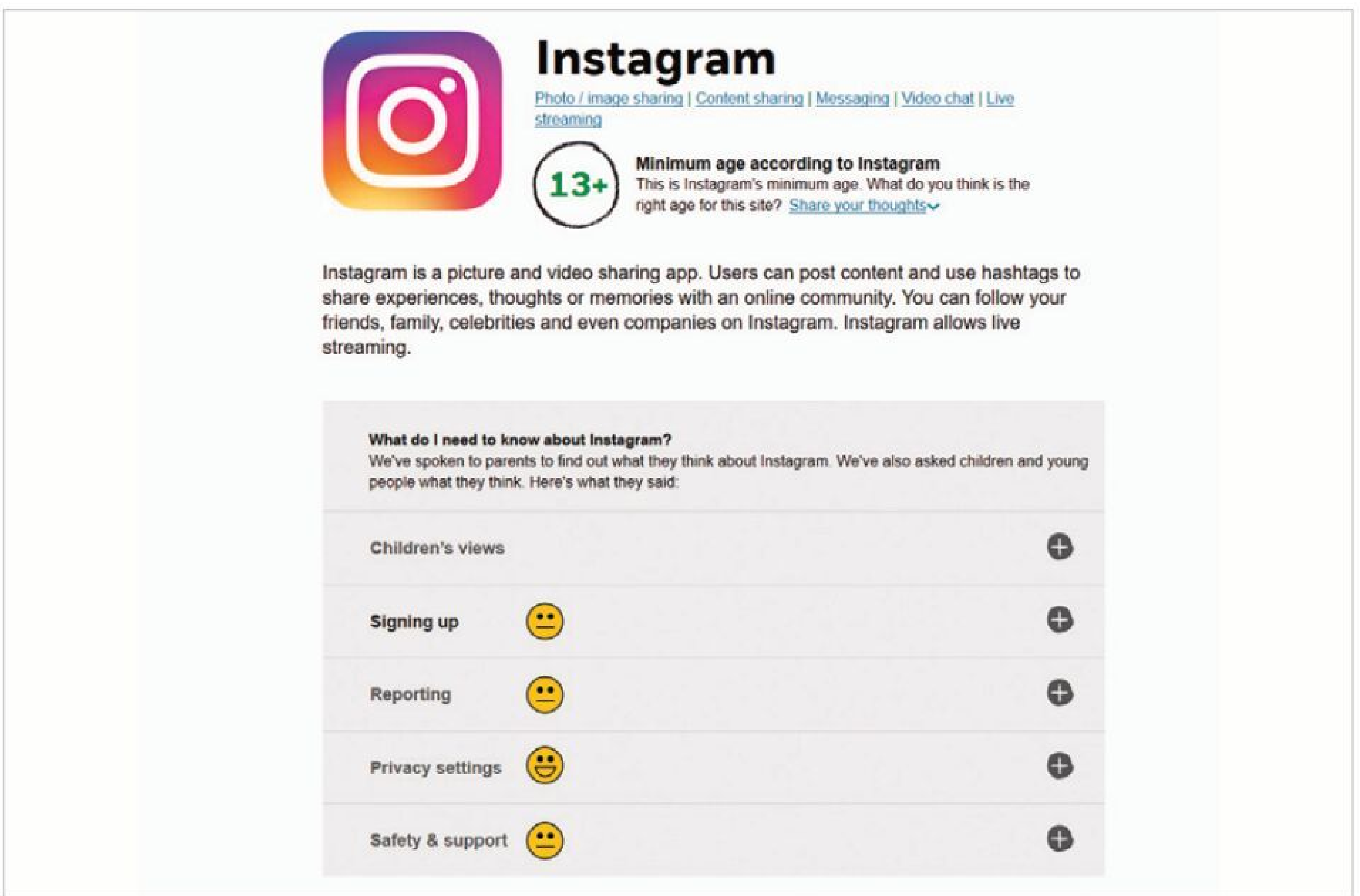
Facebook is a social network which lets you create a page about yourself. You can add friends, write on people's pages, share photos and videos including live videos. Facebook Messenger allows you to instant message in group chats or one to one. Facebook allows live streaming.

What do I need to know about Facebook and Messenger?
We've spoken to parents to find out what they think about Facebook and Messenger. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😃 ⊕
Privacy settings 😃 ⊕
Safety & support 😐 ⊕

INSTAGRAM

Instagram only manages to gain an upvote (smiley face) in the Privacy Settings section, with more rigid controls being asked for from parents and carers with regards to Signing Up, Safety & Support and Reporting.



Instagram

Photo / image sharing | Content sharing | Messaging | Video chat | Live streaming

13+ **Minimum age according to Instagram**
This is Instagram's minimum age. What do you think is the right age for this site? Share your thoughts

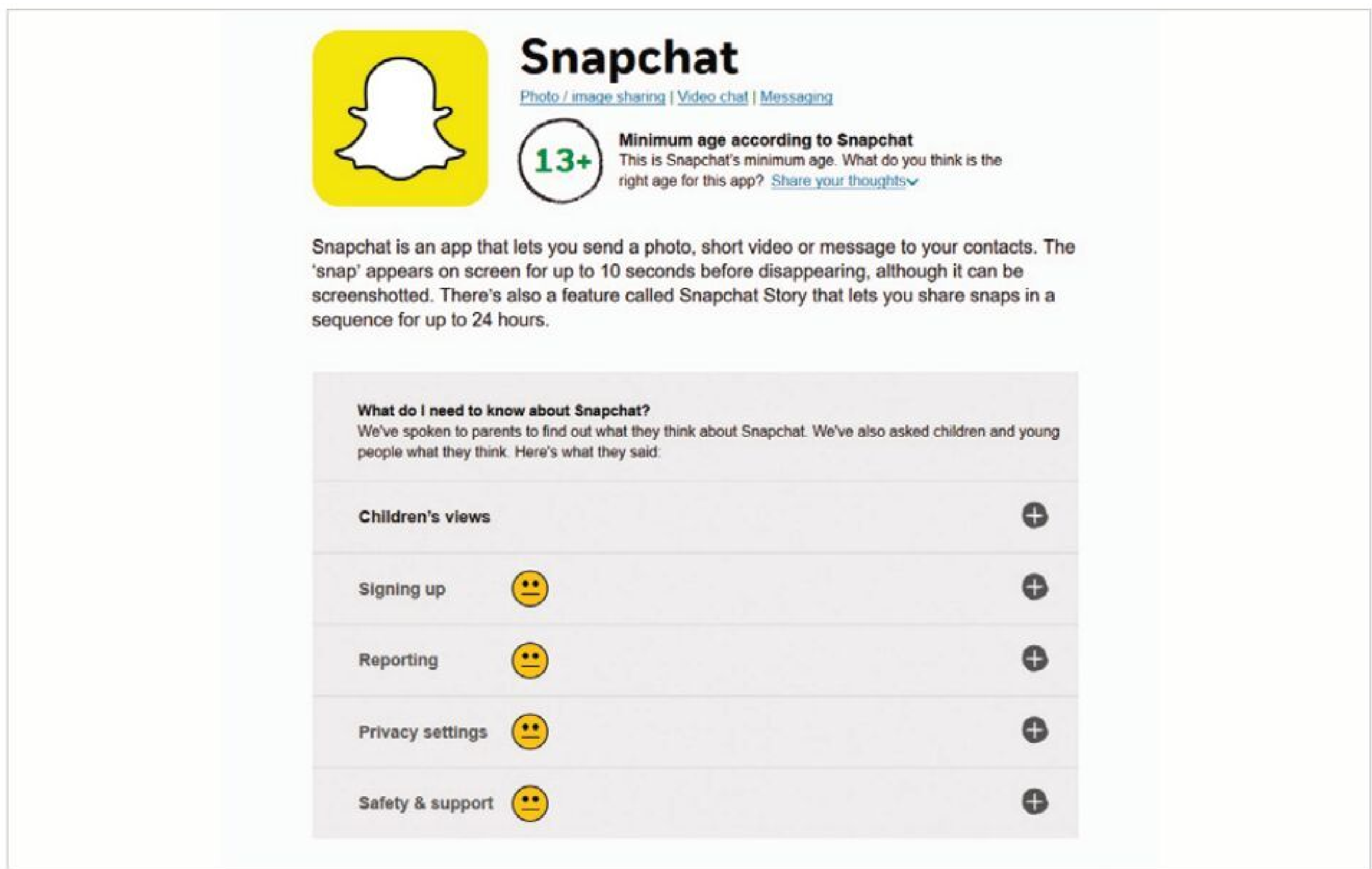
Instagram is a picture and video sharing app. Users can post content and use hashtags to share experiences, thoughts or memories with an online community. You can follow your friends, family, celebrities and even companies on Instagram. Instagram allows live streaming.

What do I need to know about Instagram?
We've spoken to parents to find out what they think about Instagram. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😃 ⊕
Safety & support 😐 ⊕

SNAPCHAT

According to Net Aware, 32% of children and young people who reviewed Snapchat thought that it can be risky. There aren't any 'happy face' icons among the sections, so be wary of how it works.



Snapchat

Photo / image sharing | Video chat | Messaging

13+ **Minimum age according to Snapchat**
This is Snapchat's minimum age. What do you think is the right age for this app? Share your thoughts

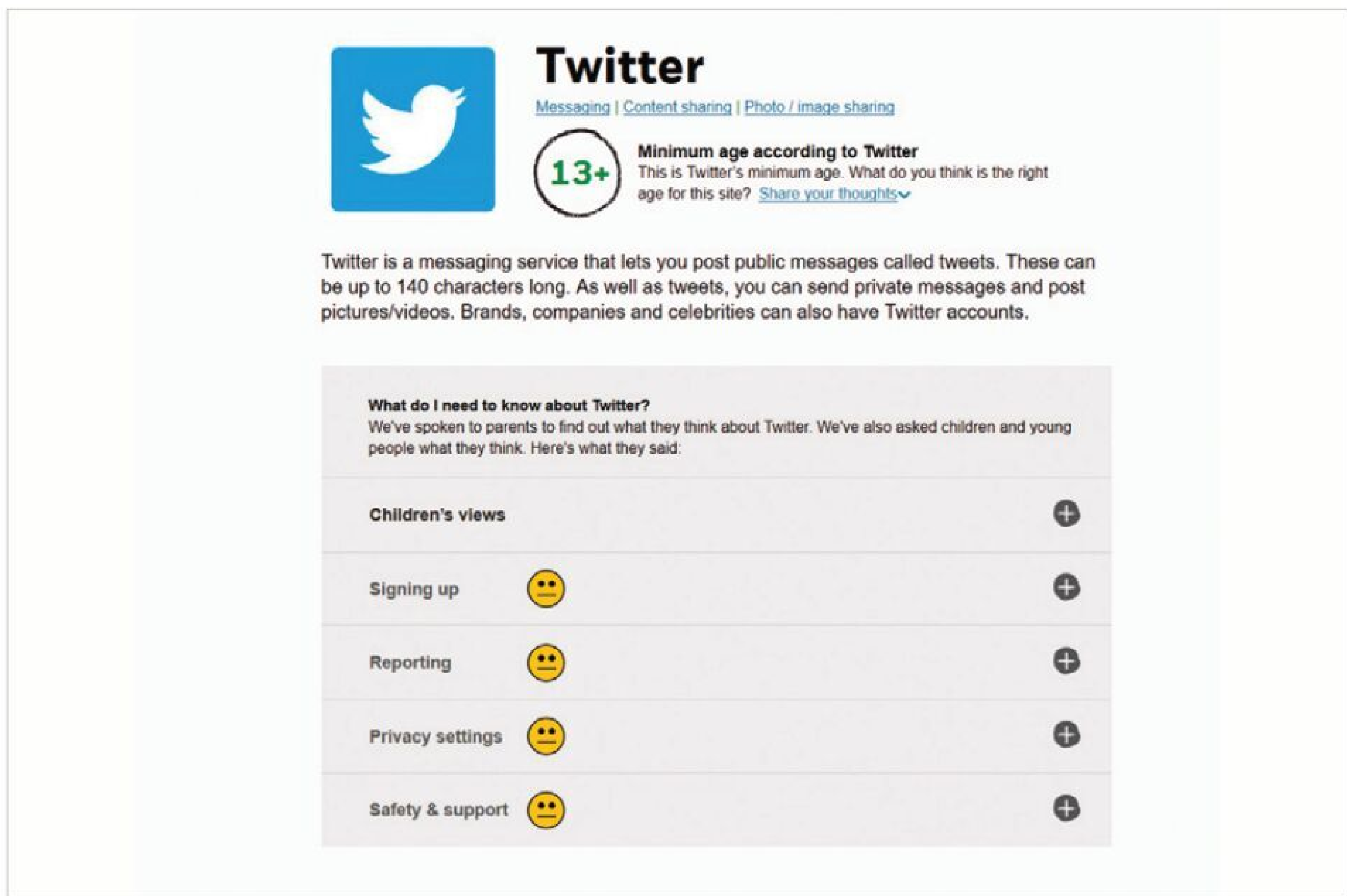
Snapchat is an app that lets you send a photo, short video or message to your contacts. The 'snap' appears on screen for up to 10 seconds before disappearing, although it can be screenshotted. There's also a feature called Snapchat Story that lets you share snaps in a sequence for up to 24 hours.

What do I need to know about Snapchat?
We've spoken to parents to find out what they think about Snapchat. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

TWITTER

Some of the major concerns regarding Twitter are: uncontrolled Tweets, fake and scam tweets and abusive behaviour. It doesn't rate too highly, on a par with Snapchat, so it's worth reading through the available content prior to signing up or allowing a young person to sign up.



Twitter

Messaging | Content sharing | Photo / image sharing

13+ **Minimum age according to Twitter**
This is Twitter's minimum age. What do you think is the right age for this site? Share your thoughts

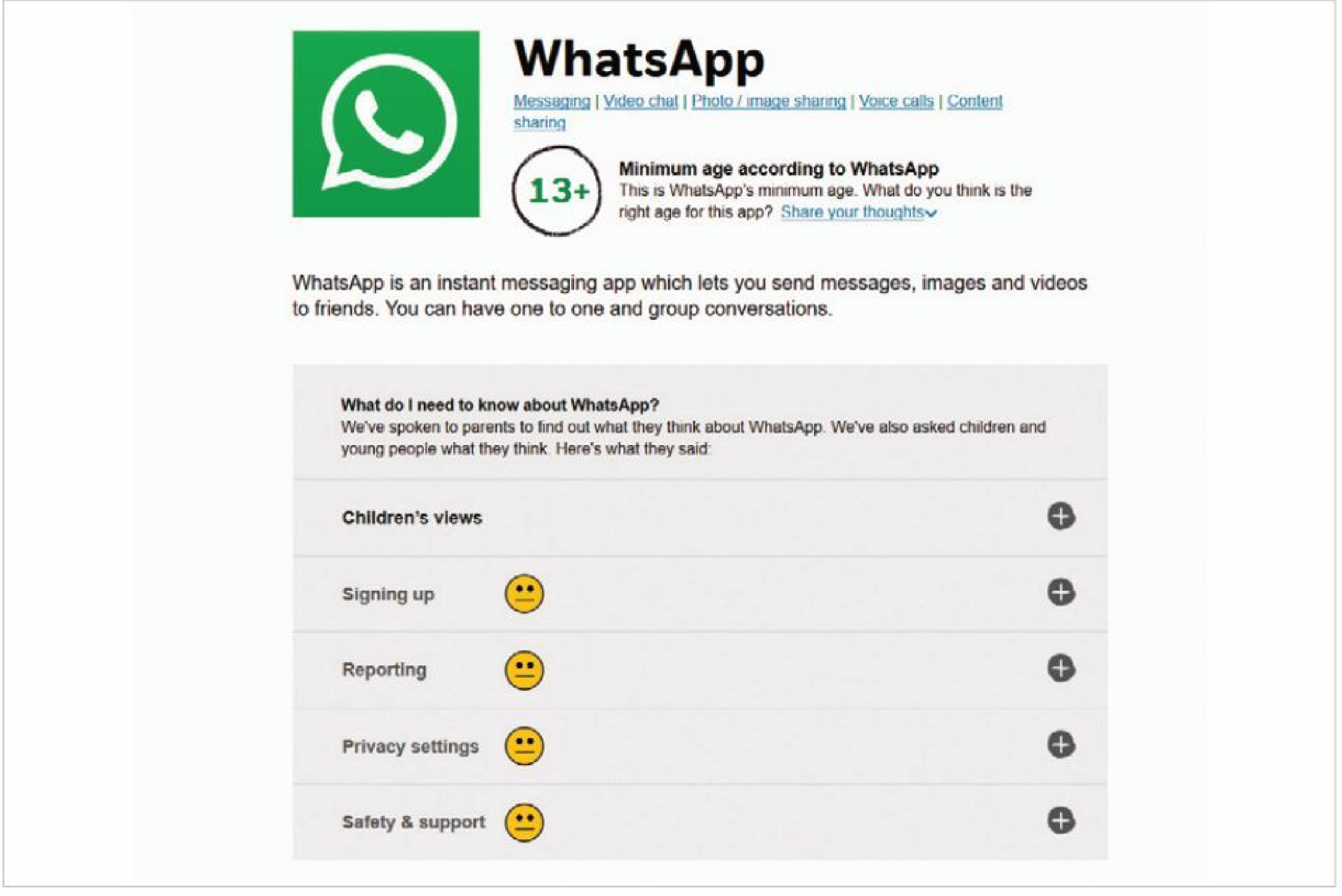
Twitter is a messaging service that lets you post public messages called tweets. These can be up to 140 characters long. As well as tweets, you can send private messages and post pictures/videos. Brands, companies and celebrities can also have Twitter accounts.

What do I need to know about Twitter?
We've spoken to parents to find out what they think about Twitter. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

WHATSAPP

Another not too highly rated site, WhatsApp raises several concerns over ability to be contacted by strangers, random people being able to view your profile picture and the potential for receiving scam messages.



WhatsApp

Messaging | Video chat | Photo / image sharing | Voice calls | Content sharing

13+ **Minimum age according to WhatsApp**
This is WhatsApp's minimum age. What do you think is the right age for this app? Share your thoughts

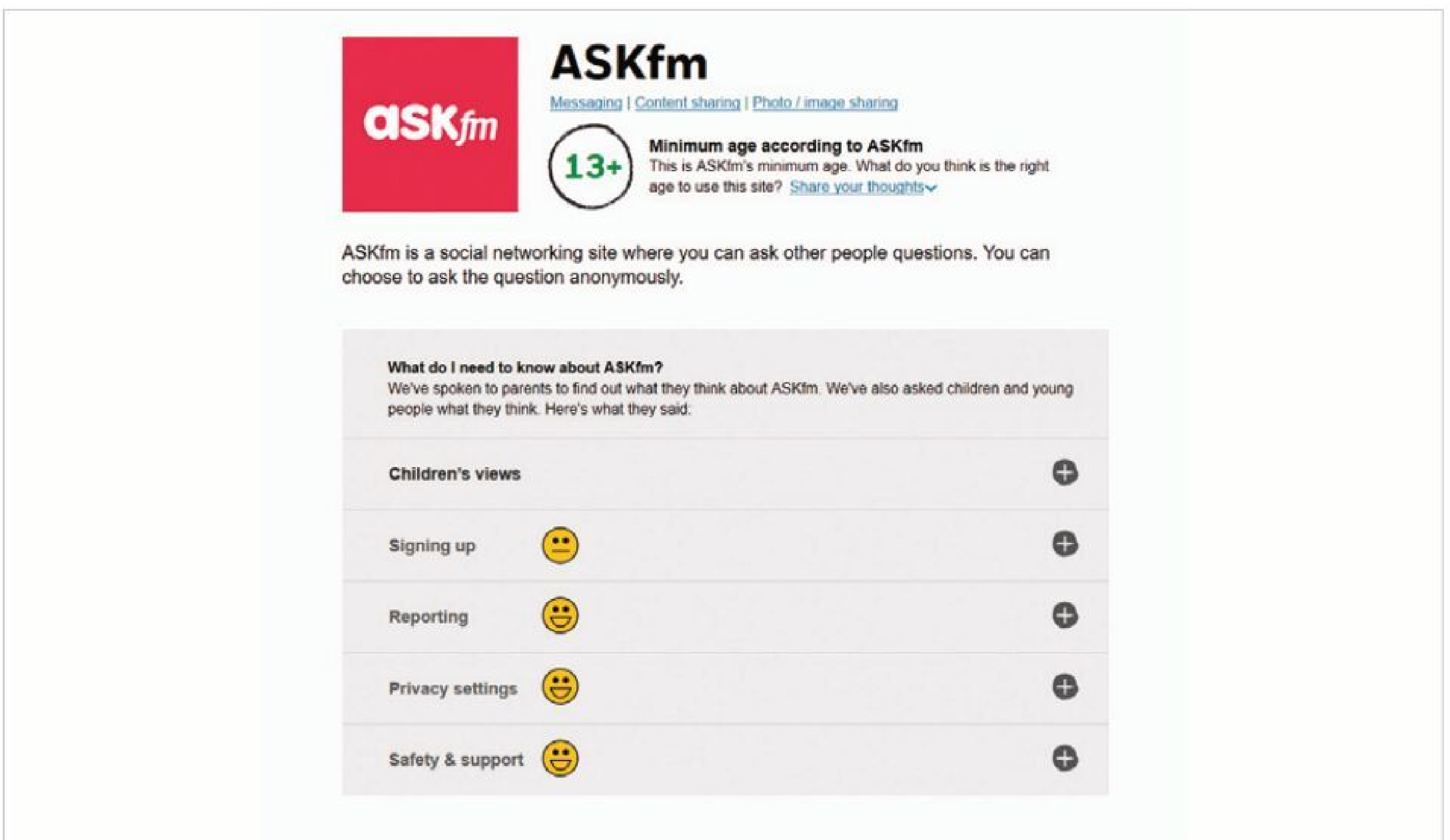
WhatsApp is an instant messaging app which lets you send messages, images and videos to friends. You can have one to one and group conversations.

What do I need to know about WhatsApp?
We've spoken to parents to find out what they think about WhatsApp. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

ASKFM

This is a social networking site where you can ask other people questions, anonymously if you want to. The anonymity raises concerns, along with instances of bullying and trolling, as well as possible exposure to inappropriate content. However, it does have the highest 'face' rating off all the apps so far.



ASKfm

Messaging | Content sharing | Photo / image sharing

13+ **Minimum age according to ASKfm**
This is ASKfm's minimum age. What do you think is the right age to use this site? Share your thoughts

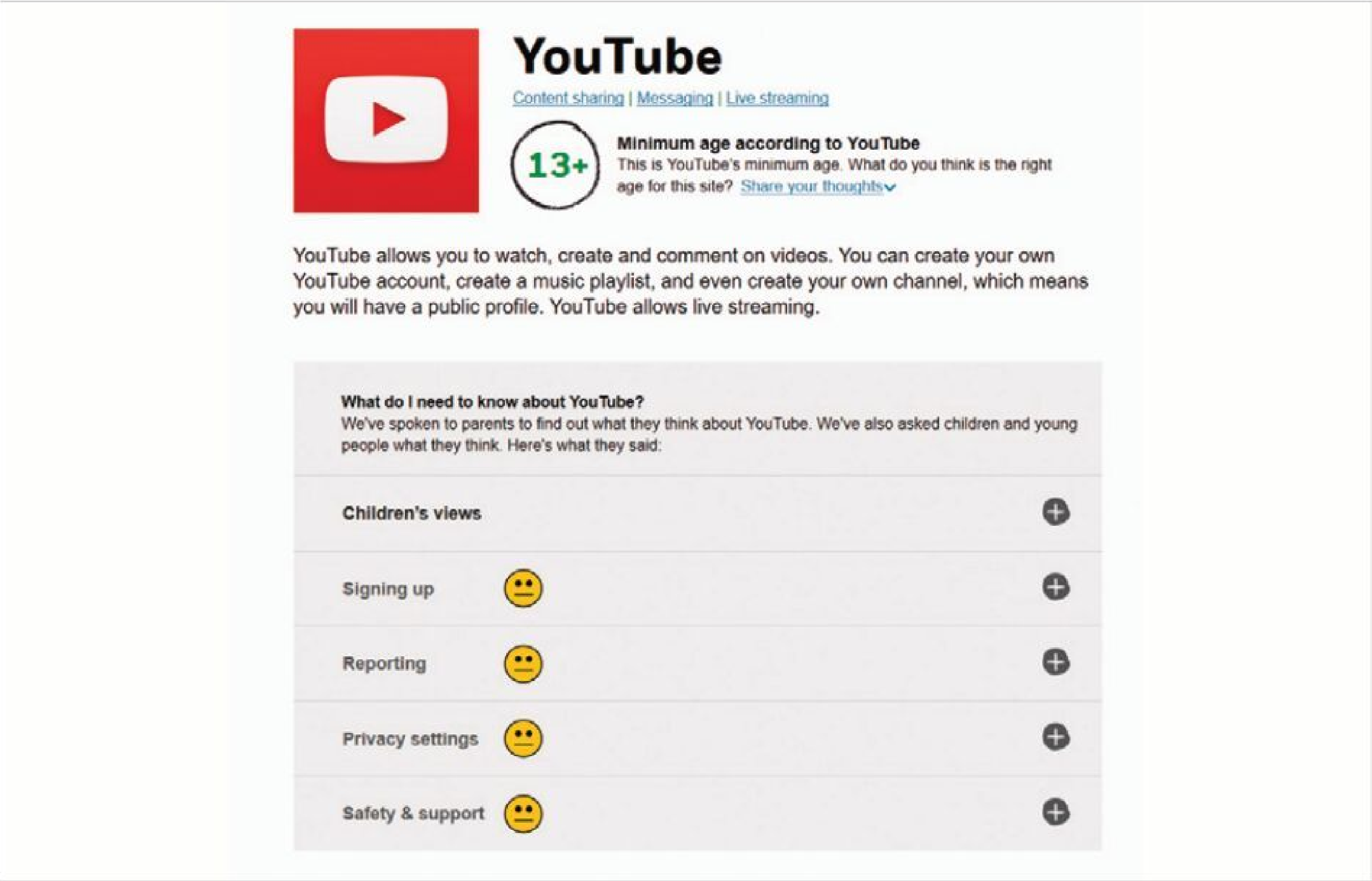
ASKfm is a social networking site where you can ask other people questions. You can choose to ask the question anonymously.

What do I need to know about ASKfm?
We've spoken to parents to find out what they think about ASKfm. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😀 ⊕
Privacy settings 😀 ⊕
Safety & support 😀 ⊕

YOUTUBE

YouTube's infamous use by extremist groups when posting inappropriate videos is by far one of the most negative aspects of its use among young people. Examples of abusive comments and possibly inappropriate adverts are concerns too. Net Aware rates it on a par with Snapchat and Twitter.



YouTube

Content sharing | Messaging | Live streaming

13+ **Minimum age according to YouTube**
This is YouTube's minimum age. What do you think is the right age for this site? Share your thoughts

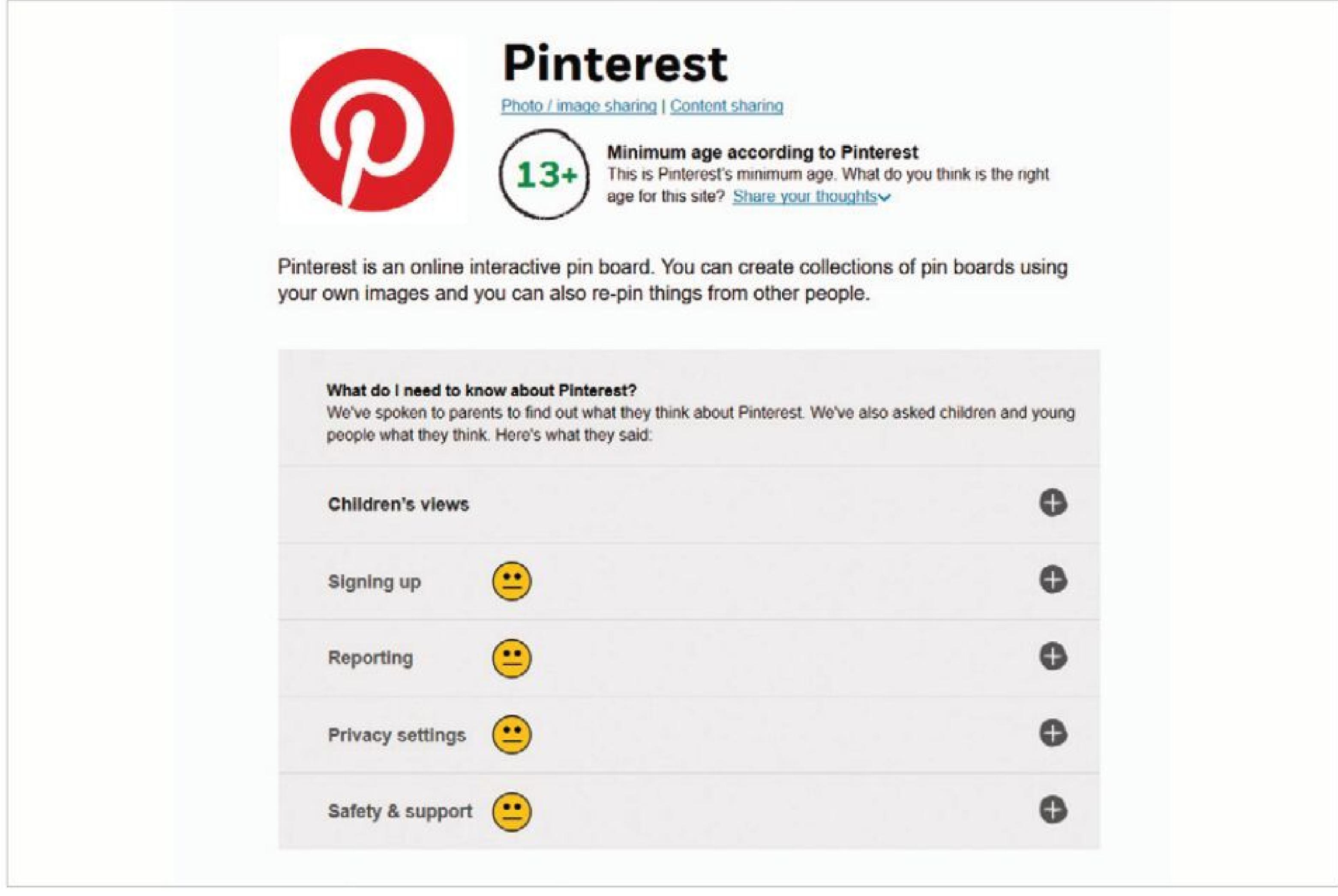
YouTube allows you to watch, create and comment on videos. You can create your own YouTube account, create a music playlist, and even create your own channel, which means you will have a public profile. YouTube allows live streaming.

What do I need to know about YouTube?
We've spoken to parents to find out what they think about YouTube. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

PINTEREST

The main concern with Pinterest is that young people and children can't always control what they see, which means there are times when inappropriate content can be viewed by minors. Again, Net Aware rate it the same as YouTube, Snapchat and Twitter.



Pinterest

Photo / image sharing | Content sharing

13+ **Minimum age according to Pinterest**
This is Pinterest's minimum age. What do you think is the right age for this site? Share your thoughts

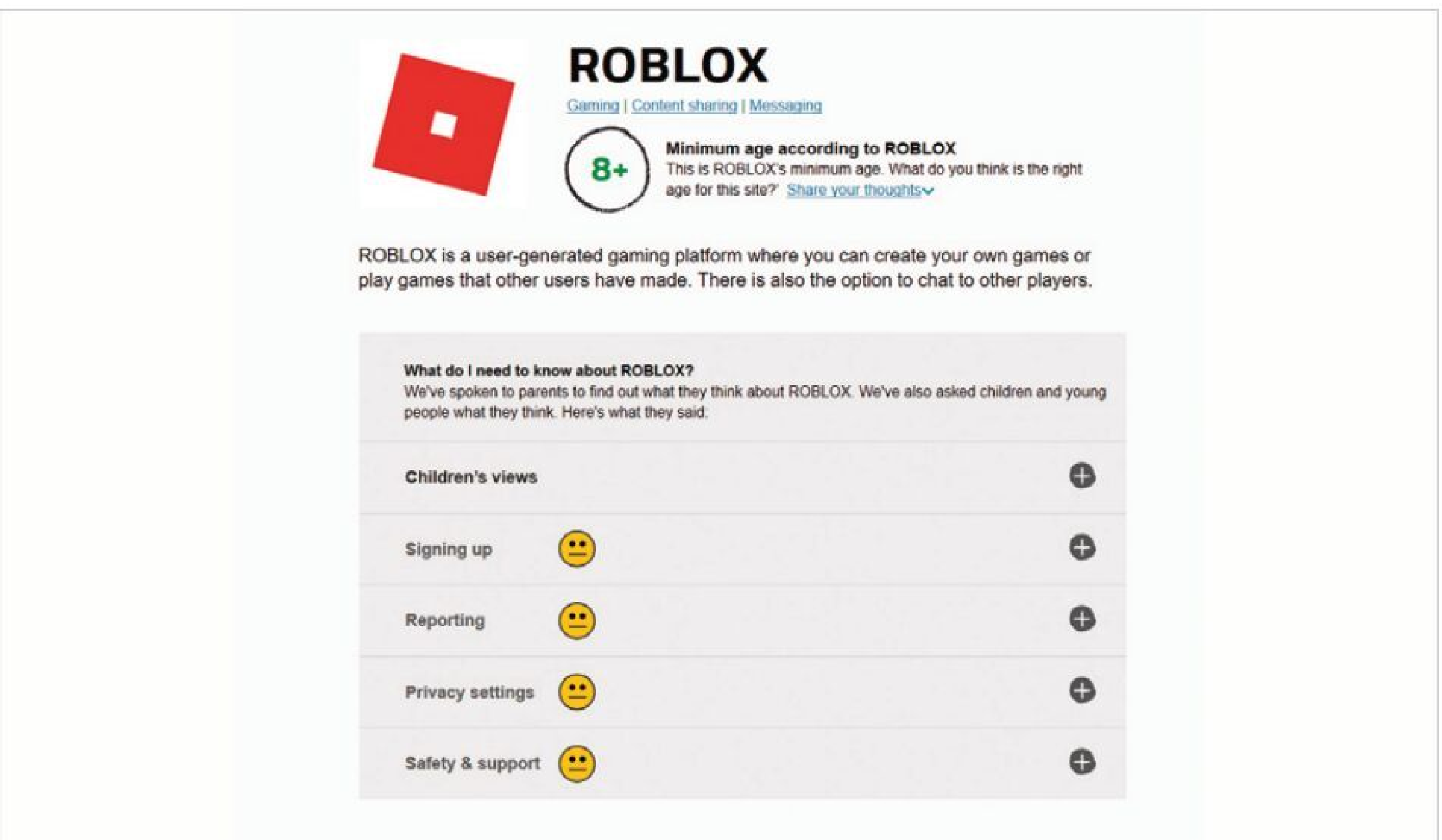
Pinterest is an online interactive pin board. You can create collections of pin boards using your own images and you can also re-pin things from other people.

What do I need to know about Pinterest?
We've spoken to parents to find out what they think about Pinterest. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

ROBLOX

This is an online game where you're able to play games created by others, or create games yourself. Whilst fun, it does have issues whereby users can add you to their friends list and communicate with you and it features in-app purchasing, which can be difficult to manage for parents and guardians.



ROBLOX

Gaming | Content sharing | Messaging

8+ **Minimum age according to ROBLOX**
This is ROBLOX's minimum age. What do you think is the right age for this site?' Share your thoughts

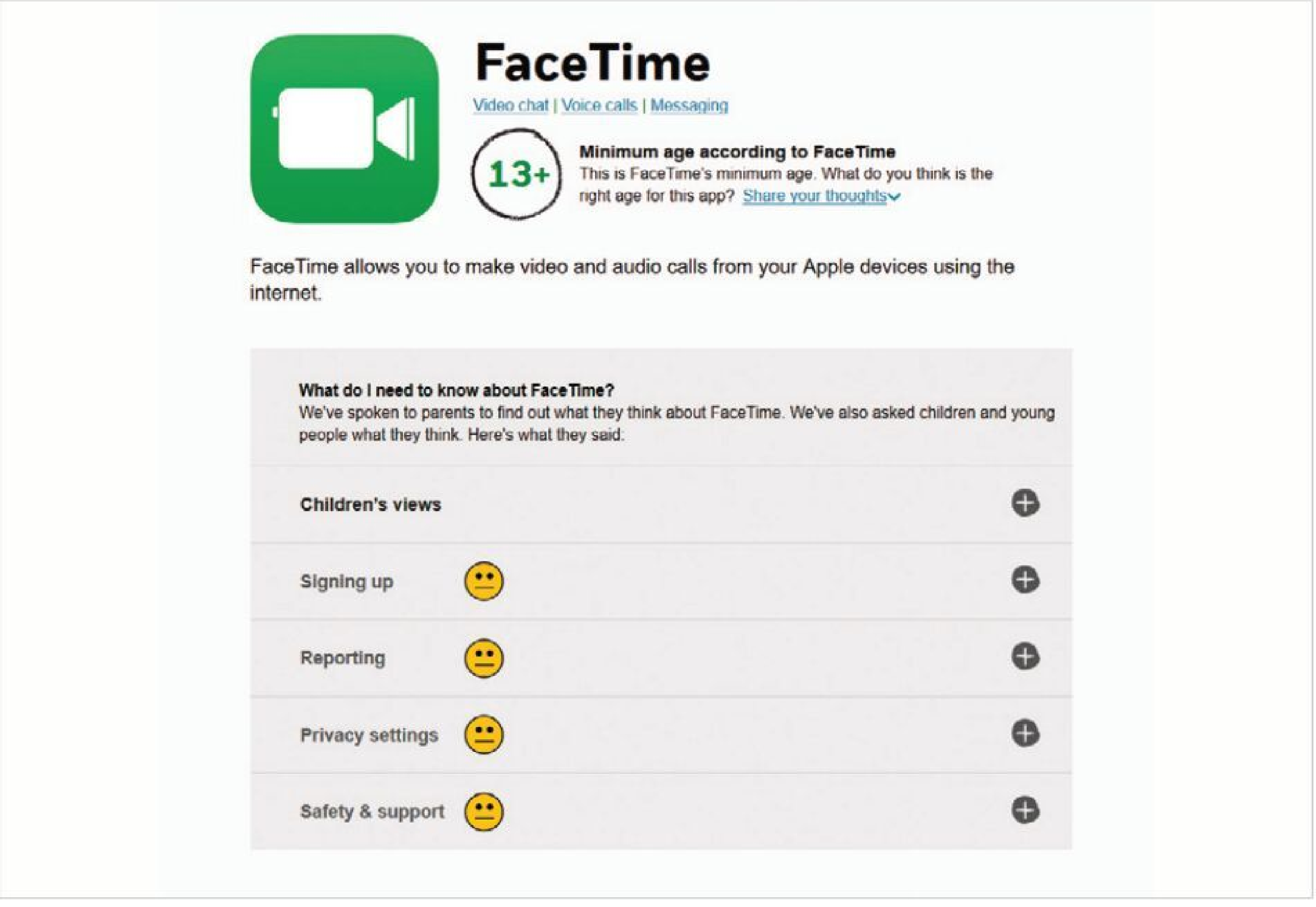
ROBLOX is a user-generated gaming platform where you can create your own games or play games that other users have made. There is also the option to chat to other players.

What do I need to know about ROBLOX?
We've spoken to parents to find out what they think about ROBLOX. We've also asked children and young people what they think. Here's what they said.

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

FACETIME

Apple's FaceTime is one of the most used video chat clients available. However, it has been noted that people you don't know can FaceTime you and it's possible to record or take screen shots of a FaceTime conversation without you knowing.



FaceTime

Video chat | Voice calls | Messaging

13+ **Minimum age according to FaceTime**
This is FaceTime's minimum age. What do you think is the right age for this app? Share your thoughts

FaceTime allows you to make video and audio calls from your Apple devices using the internet.

What do I need to know about FaceTime?
We've spoken to parents to find out what they think about FaceTime. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

Email & Child

We're often so concerned over social media, online gaming and chat sites that we tend to ignore one of the most common threats to online safety for young people and children, email. While it's a more manageable element, it does carry plenty of dangerous potential.

In reality it doesn't take too much of a technical genius to enter into a search engine, "fake email accounts" or something similar. The returned results, such as Fake Email Generator, Mailinator, ThrowAwayMail and FakeInbox are all designed to help you create a fake account that can either be single use or used regularly. This of course means that a person is able to create a false persona and sign up for Facebook and the like using a browser's private function, and have access to accounts without someone else knowing.

This works both ways, from the point of view of the young person gaining access to a site they shouldn't and for someone who's creating accounts ready for grooming, or something similar. With access to a fake email, a young person has the potential get into a variety of potential dangerous situations. They could be contacted by someone who is trying to groom or send radicalised content, they could also become the subject of a hack and unwittingly execute code that can deploy a virus, ransomware or other malware, along with possible backdoor hacks to gain access to the system the young person is using.

It's not just fake email sites that pose a danger when it comes to young people and children; although fake email sites usually don't have the better protection and anti-malware restrictions that more legitimate sites employ. Google Mail, Yahoo and so on can represent a weak link in the chain of digital protection for children and young people. The dangers are mostly the same but thankfully these online mail providers have better levels of malware protection.

So how would you, as a parent or guardian, combat potential email threats for children and young people? You may not be able to police their mobile accounts all the time but you can insist that they allow you access to the account on a regular basis to check that they're not in conversation with someone unknown, or that they're not receiving and responding to reams of spam and malware ridden emails. However, that does seem something of an Orwellian approach to managing a young person's email account.

Another possibility is to set up a family email account, separate from the parents or guardians' accounts, where the entire family has access and can utilise to sign up for games, safe sites and the like. It's a more open approach, whilst still preserving privacy for the adults and if you use folders within the email client or website, then there's some privacy for the young person too.

Naturally the best form of email attack and threat prevention is through education. Both the NSPCC and Childline recommend that you talk to your child and come up with a set of workable rules and conditions that are fair but protective. Educate them on the dangers of communicating with a stranger and inform them that online grooming takes place and how it works, also include how viruses work and other forms of malware, and how phishing and other forms of threats work too.

There are some tips that we as parents or guardians can use to help children and young people:

- Treat all people on the Internet as strangers, even those who could be friends.
- Never give out any personal information via email to an unknown source or site.
- Be wary when choosing an email name, don't use anything to identify your gender or anything provocative.
- Never open an email attachment. Check with a parent or guardian first.
- Never reply to an unknown email and never send any images of yourself.
- Always tell a parent, guardian or teacher if you've been contacted by someone you don't know.
- Never respond to a threating email or someone attempting to bait you into contact.
- Don't always believe everything you read in an email. Phishing attempts come as virus hoaxes.
- Don't believe you've won £1,000,000 or react to limited time ridiculous offers on technology or fashion. It's nearly always fake emails trying to get you to visit a site.

Another possibility is to use one of the many child friendly email programs and online services. There are ample available to try out and over the next couple of pages we take a look at ten of the more highly recommended services.

"Email Risks"

Email at first doesn't appear to be too much of a concern for the parent or guardian, after all we can view what emails are coming in to our accounts. However, it's not too difficult for a tech-savvy youngster to create an alternative email account, usually one that's web-based, that they can use to access games and sites you wouldn't normally allow them to.

Safety

Top Child Friendly Email Programs and Services

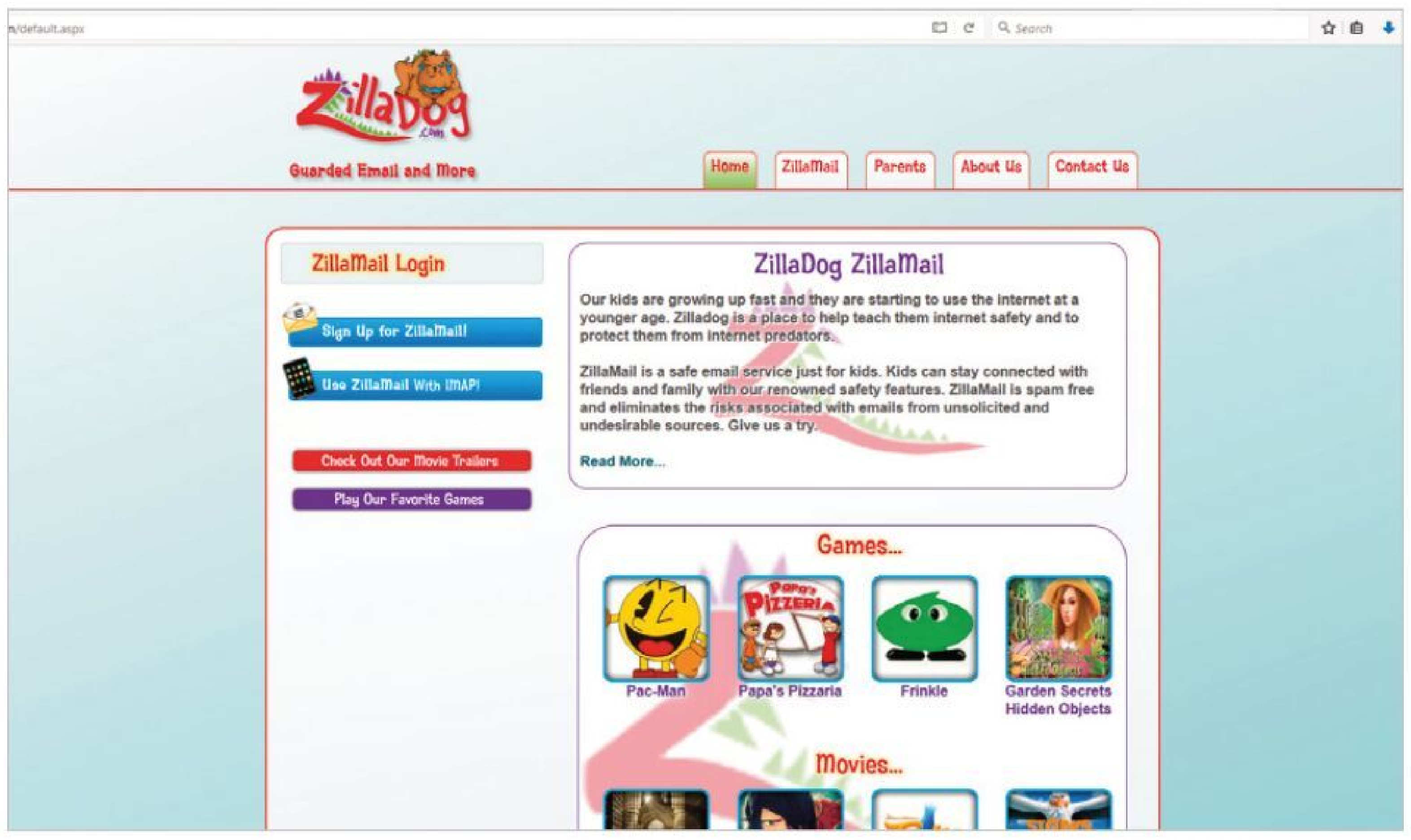
An email account for a child or young person is a great way for them to communicate with friends and family; however, as we've seen, it can be a dangerous tool. Therefore it's best to ensure they're using a safe, child friendly email account.

Ten Child Safe Email Accounts

It's not always easy to police and monitor an email account, so here are ten child friendly email accounts and related services that will help make the job of keeping children safer when communicating via email.

ZILLAMAIL

ZillaMail is run under the ZillaDog.com brand, created by parents for children. It's an easy to use, friendly service that also combines child safe online games and links to child safe websites, such as Cartoon Network and the like. ZillaMail has some interesting aspects and features, which makes it an excellent choice for parents and guardians.


n/default.aspx
Search
ZillaDog.com
Guarded Email and More
Home
ZillaMail
Parents
About Us
Contact Us
ZillaMail Login
Sign Up for ZillaMail!
Use ZillaMail With IMAP!
Check Out Our Movie Trailers
Play Our Favorite Games
Games...
Pac-Man
Papa's Pizzaria
Frinkle
Garden Secrets Hidden Objects
Movies...

ZillaDog ZillaMail

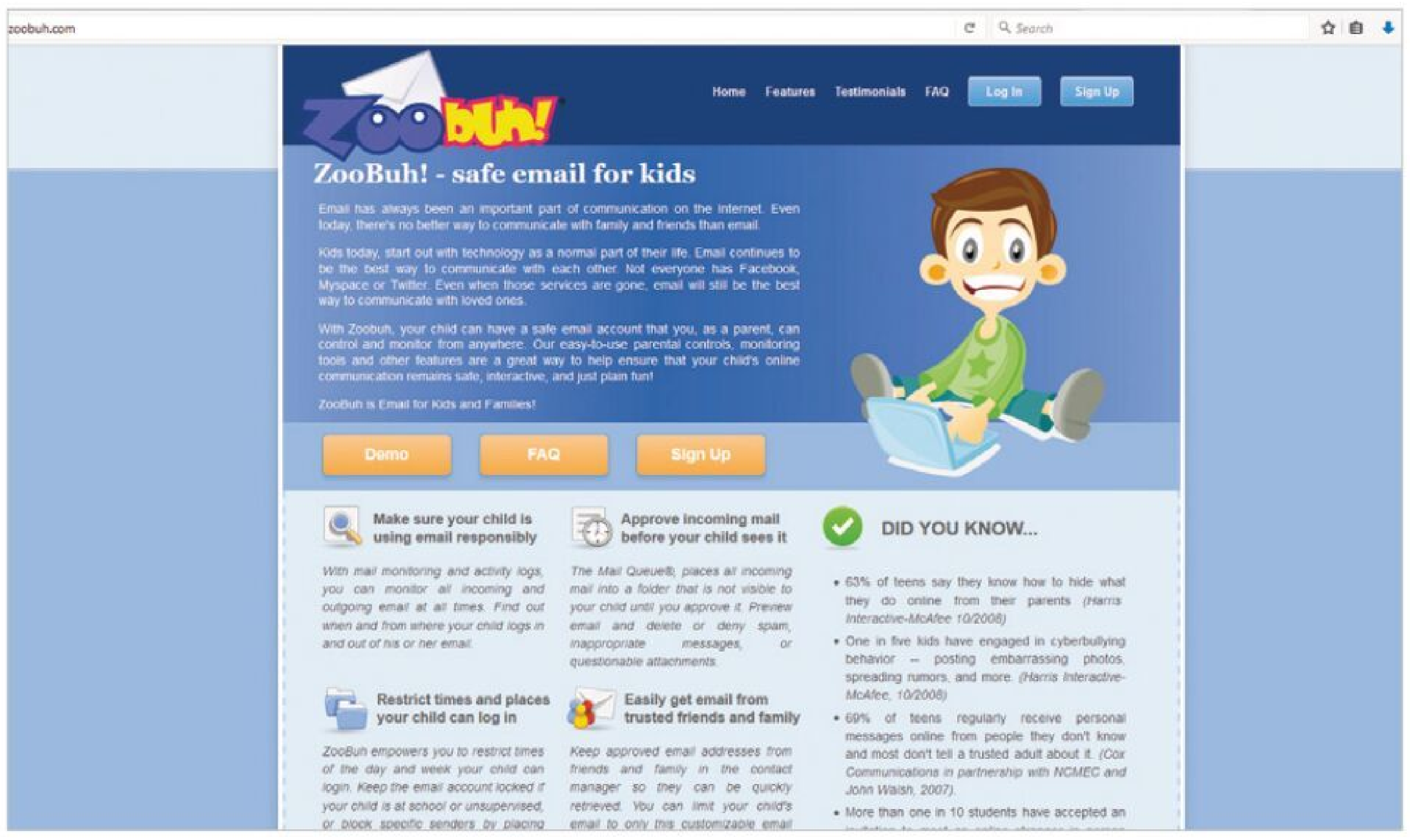
Our kids are growing up fast and they are starting to use the internet at a younger age. Zilladog is a place to help teach them internet safety and to protect them from internet predators.

ZillaMail is a safe email service just for kids. Kids can stay connected with friends and family with our renowned safety features. ZillaMail is spam free and eliminates the risks associated with emails from unsolicited and undesirable sources. Give us a try.

Read More...

ZOOBUH

ZooBuh has an impressive list of benefits and features for parents and guardians to look over when considering an email provider for their child. Adjustable spam filtering, the ability to delete attachments, block specific senders, see activity logs and a Predator Catch Phrase alert system all add up to a great service.


zoobuh.com
Search
ZooBuh!
Home
Features
Testimonials
FAQ
Log In
Sign Up
Demo
FAQ
Sign Up

ZooBuh! - safe email for kids

Email has always been an important part of communication on the internet. Even today, there's no better way to communicate with family and friends than email.

Kids today, start out with technology as a normal part of their life. Email continues to be the best way to communicate with each other. Not everyone has Facebook, Myspace or Twitter. Even when those services are gone, email will still be the best way to communicate with loved ones.

With Zoobuh, your child can have a safe email account that you, as a parent, can control and monitor from anywhere. Our easy-to-use parental controls, monitoring tools and other features are a great way to help ensure that your child's online communication remains safe, interactive, and just plain fun!

ZooBuh is Email for Kids and Families!

Make sure your child is using email responsibly

With mail monitoring and activity logs, you can monitor all incoming and outgoing email at all times. Find out when and from where your child logs in and out of his or her email.

Approve incoming mail before your child sees it

The Mail Queue®, places all incoming mail into a folder that is not visible to your child until you approve it. Preview email and delete or deny spam, inappropriate messages, or questionable attachments.

Restrict times and places your child can log in

ZooBuh empowers you to restrict times of the day and week your child can login. Keep the email account locked if your child is at school or unsupervised, or block specific senders by placing

Easily get email from trusted friends and family

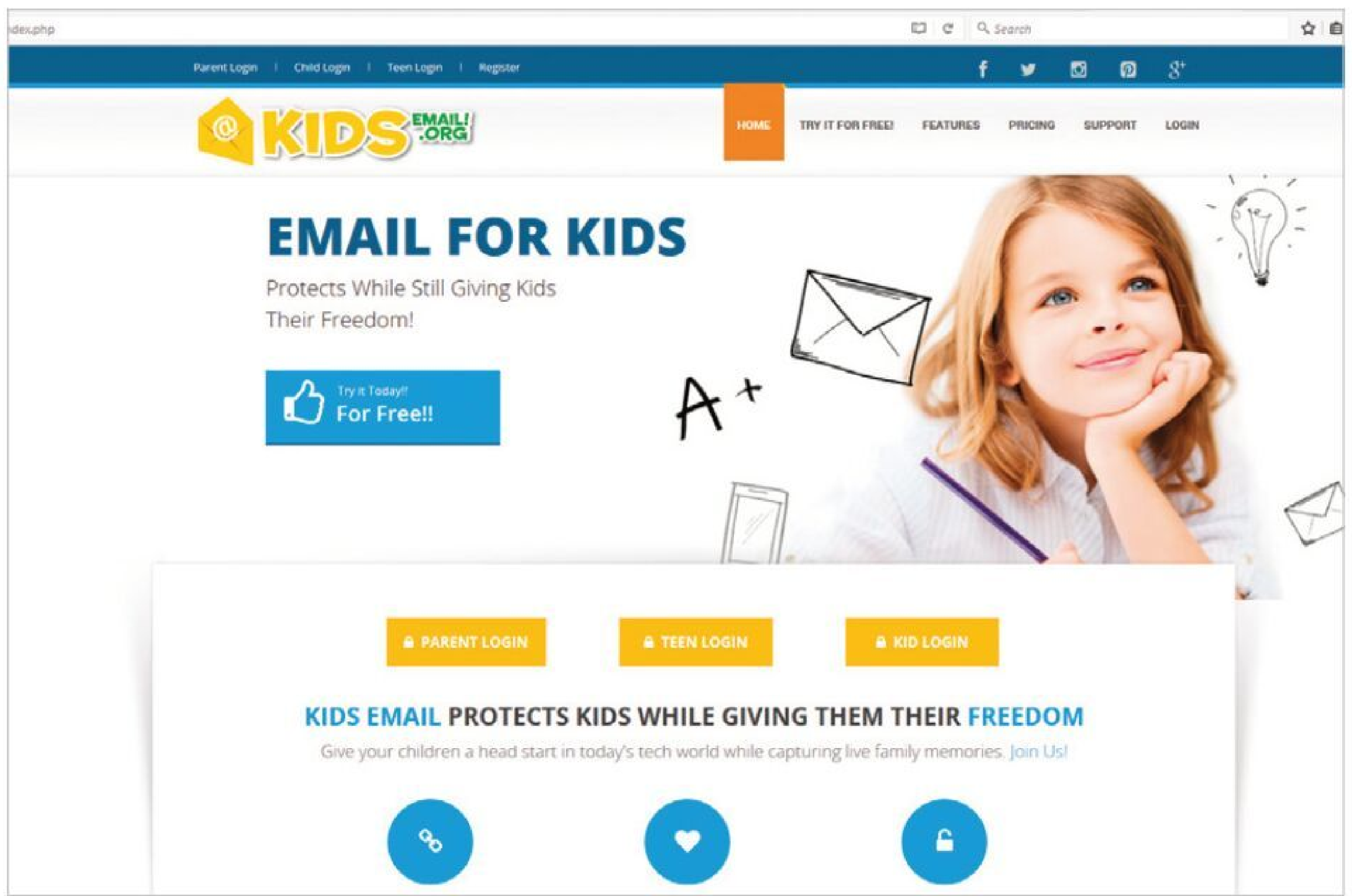
Keep approved email addresses from friends and family in the contact manager so they can be quickly retrieved. You can limit your child's email to only this customizable email

DID YOU KNOW...

- 63% of teens say they know how to hide what they do online from their parents *(Harris Interactive-McAfee 10/2008)*
- One in five kids have engaged in cyberbullying behavior – posting embarrassing photos, spreading rumors, and more. *(Harris Interactive-McAfee, 10/2008)*
- 69% of teens regularly receive personal messages online from people they don't know and most don't tell a trusted adult about it. *(Cox Communications in partnership with NCMEC and John Walsh, 2007)*
- More than one in 10 students have accepted an

KIDSEMAIL

KidsEmail is a paid for service, offering a 30 day free trial period. For your money you get mail monitoring for all incoming and outgoing emails from the child's account, time restrictions, blocked senders, no adverts, spam filtering and an easy way to add friends and family contact details.


dex.php
Search
Parent Login | Child Login | Teen Login | Register
KIDS EMAIL!.ORG
HOME
TRY IT FOR FREE!
FEATURES
PRICING
SUPPORT
LOGIN
Try it Today!!
For Free!!
A+
PARENT LOGIN
TEEN LOGIN
KID LOGIN

EMAIL FOR KIDS

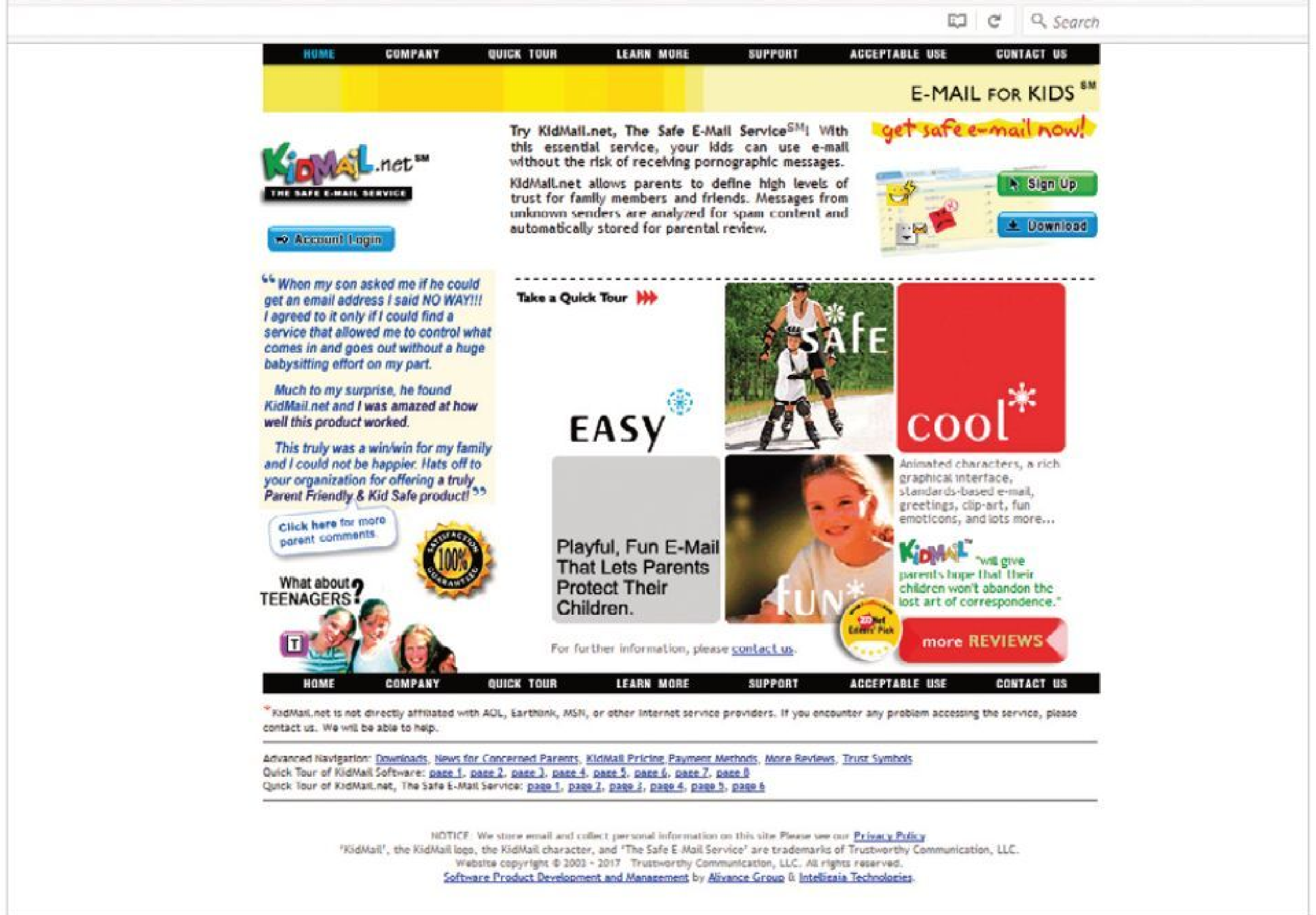
Protects While Still Giving Kids Their Freedom!

KIDS EMAIL PROTECTS KIDS WHILE GIVING THEM THEIR FREEDOM

Give your children a head start in today's tech world while capturing live family memories. Join Us!

KIDMAIL

KidMail is a low cost subscription email service that caters for both young children and older young people. Parents and guardians have full control over the email account and the messages that come and go from the child's account, along with many other benefits and features.


Search
HOME
COMPANY
QUICK TOUR
LEARN MORE
SUPPORT
ACCEPTABLE USE
CONTACT US
E-MAIL FOR KIDS SM
KidMaiL.net SM
THE SAFE E-MAIL SERVICE
get safe e-mail now!
Sign Up
Download
Account Login
Take a Quick Tour
safe
cool
EASY
fun
Click here for more parent comments
100% SATISFACTION GUARANTEED
What about TEENAGERS?
more REVIEWS
HOME
COMPANY
QUICK TOUR
LEARN MORE
SUPPORT
ACCEPTABLE USE
CONTACT US

Try KidMail.net, The Safe E-Mail Service^{SM}! With this essential service, your kids can use e-mail without the risk of receiving pornographic messages.

KidMail.net allows parents to define high levels of trust for family members and friends. Messages from unknown senders are analyzed for spam content and automatically stored for parental review.

"When my son asked me if he could get an email address I said NO WAY!!! I agreed to it only if I could find a service that allowed me to control what comes in and goes out without a huge babysitting effort on my part.

Much to my surprise, he found KidMail.net and I was amazed at how well this product worked.

This truly was a win/win for my family and I could not be happier. Hats off to your organization for offering a truly Parent Friendly & Kid Safe product!"

Playful, Fun E-Mail That Lets Parents Protect Their Children.

Animated characters, a rich graphical interface, standards-based e-mail, greetings, clip-art, fun emoticons, and lots more...

KidMail "will give parents hope that their children won't abandon the lost art of correspondence."

For further information, please contact us.

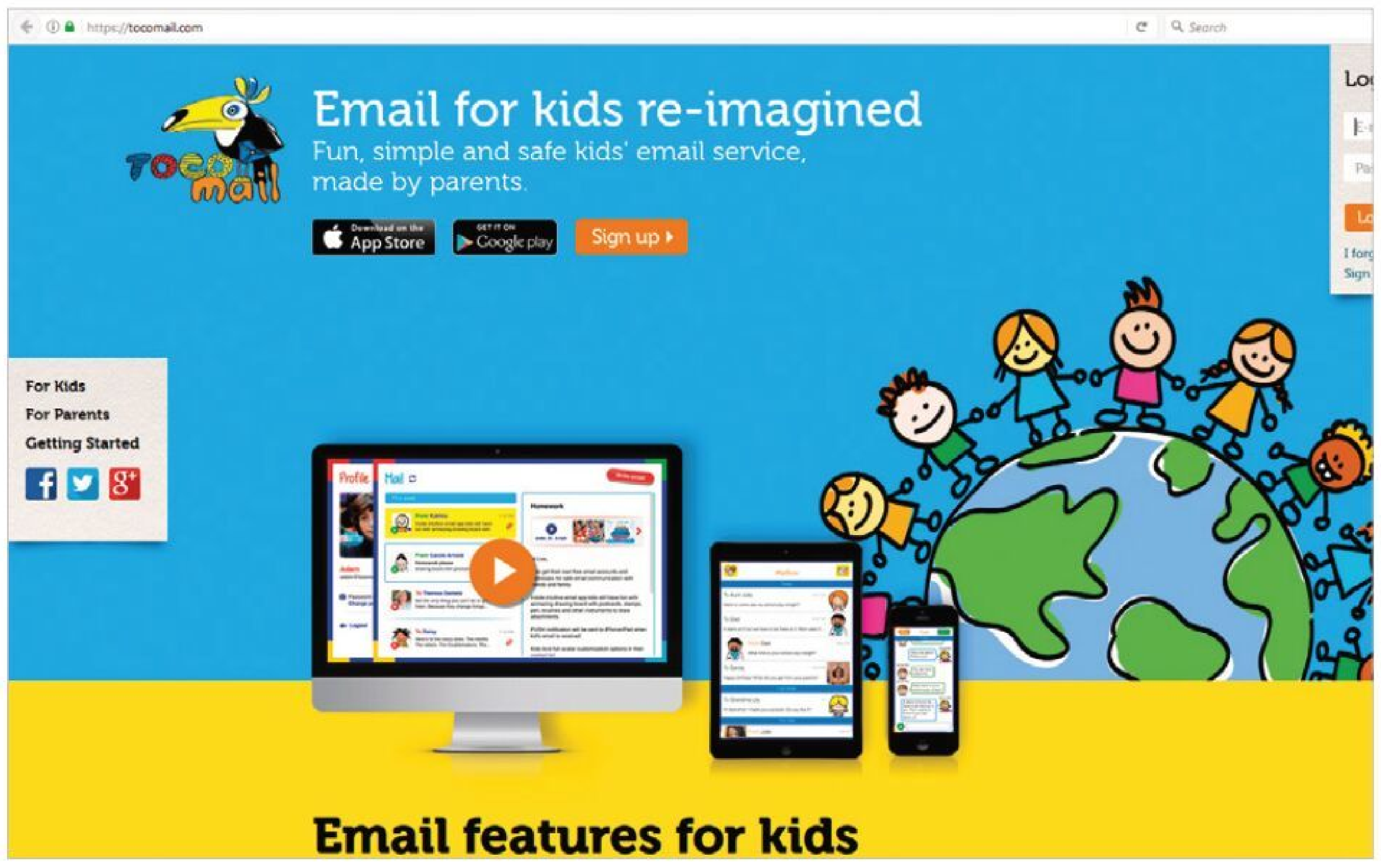
*KidMail.net is not directly affiliated with AOL, Earthlink, MSN, or other Internet service providers. If you encounter any problem accessing the service, please contact us. We will be able to help.

Advanced Navigation: Downloads, News for Concerned Parents, KidMail Pricing Payment Methods, More Reviews, Trust Symbols
Quick Tour of KidMail Software: page 1, page 2, page 3, page 4, page 5, page 6, page 7, page 8
Quick Tour of KidMail.net, The Safe E-Mail Service: page 1, page 2, page 3, page 4, page 5, page 6

NOTICE: We store email and collect personal information on this site. Please see our Privacy Policy.
"KidMail", the KidMail logo, the KidMail character, and "The Safe E-Mail Service" are trademarks of Trustworthy Communication, LLC.
Website copyright © 2003 - 2017 Trustworthy Communication, LLC. All rights reserved.
Software Product Development and Management by Alivance Group & Intelligaia Technologies.

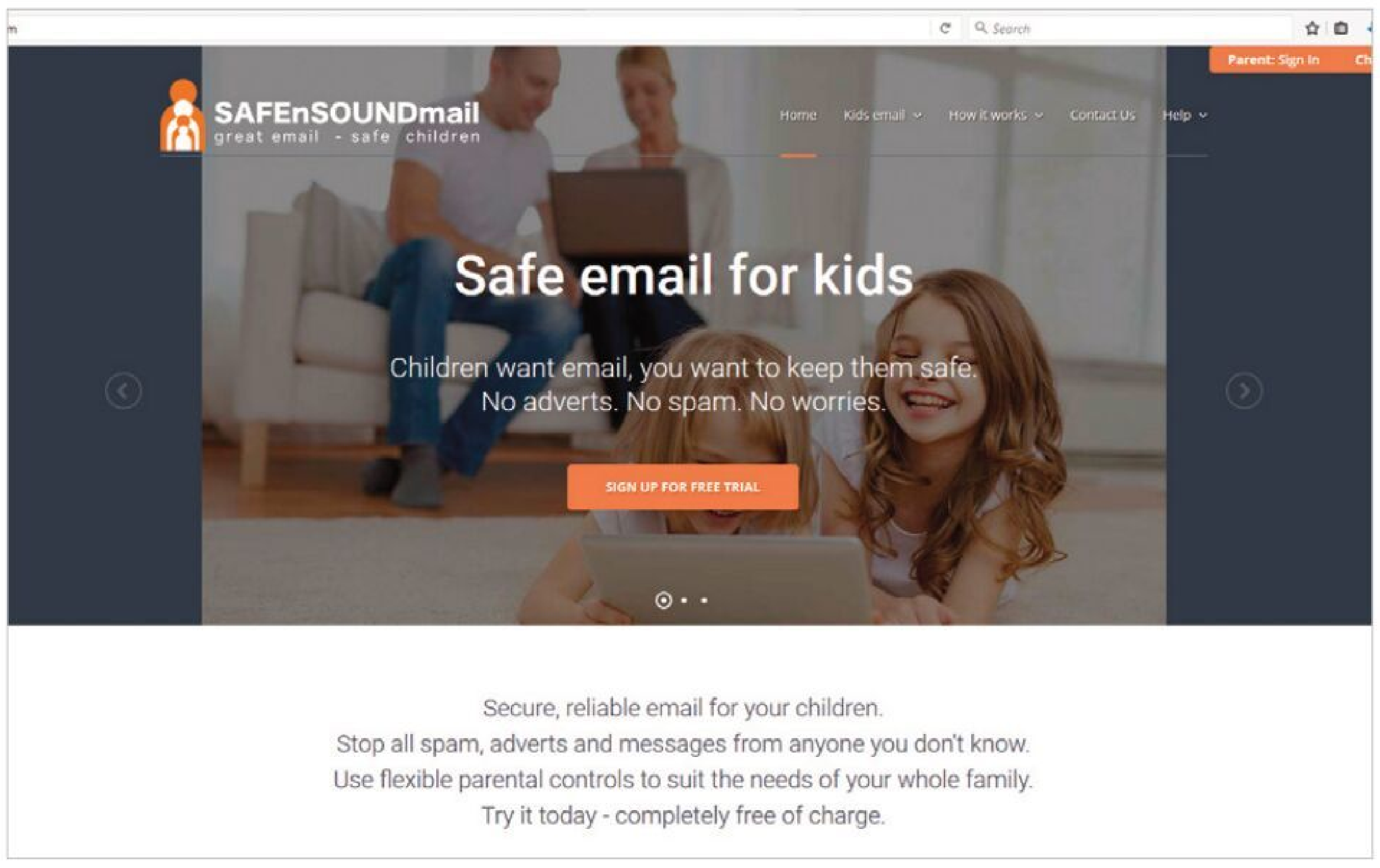
TOCOMAIL

Another well presented service, Tocomail offers the child, parent and guardian a wealth of fun and useful features. It brings a lot more than just email to the table, for example children get access to a drawing board app, to create their own attachments, whilst parents get notifications via an app when the child has received an email.


https://tocomail.com
Email for kids re-imagined
Fun, simple and safe kids' email service, made by parents.
App Store
Google play
Sign up
For Kids
For Parents
Getting Started
Email features for kids

SAFENSOUNDMAIL

SAFEnSOUNDmail has plenty of features available to those who purchase the subscription; however, there's a free 30-day trial to begin with. There's support for Apple, Android, Windows, Mac and Chromebook devices, up to five child accounts available, customisable controls and settings and elevated levels of encryption.


SAFEnSOUNDmail
great email - safe children
Home
Kids email
How it works
Contact Us
Help
Parent: Sign In
Safe email for kids
SIGN UP FOR FREE TRIAL

Children want email, you want to keep them safe.
No adverts. No spam. No worries.

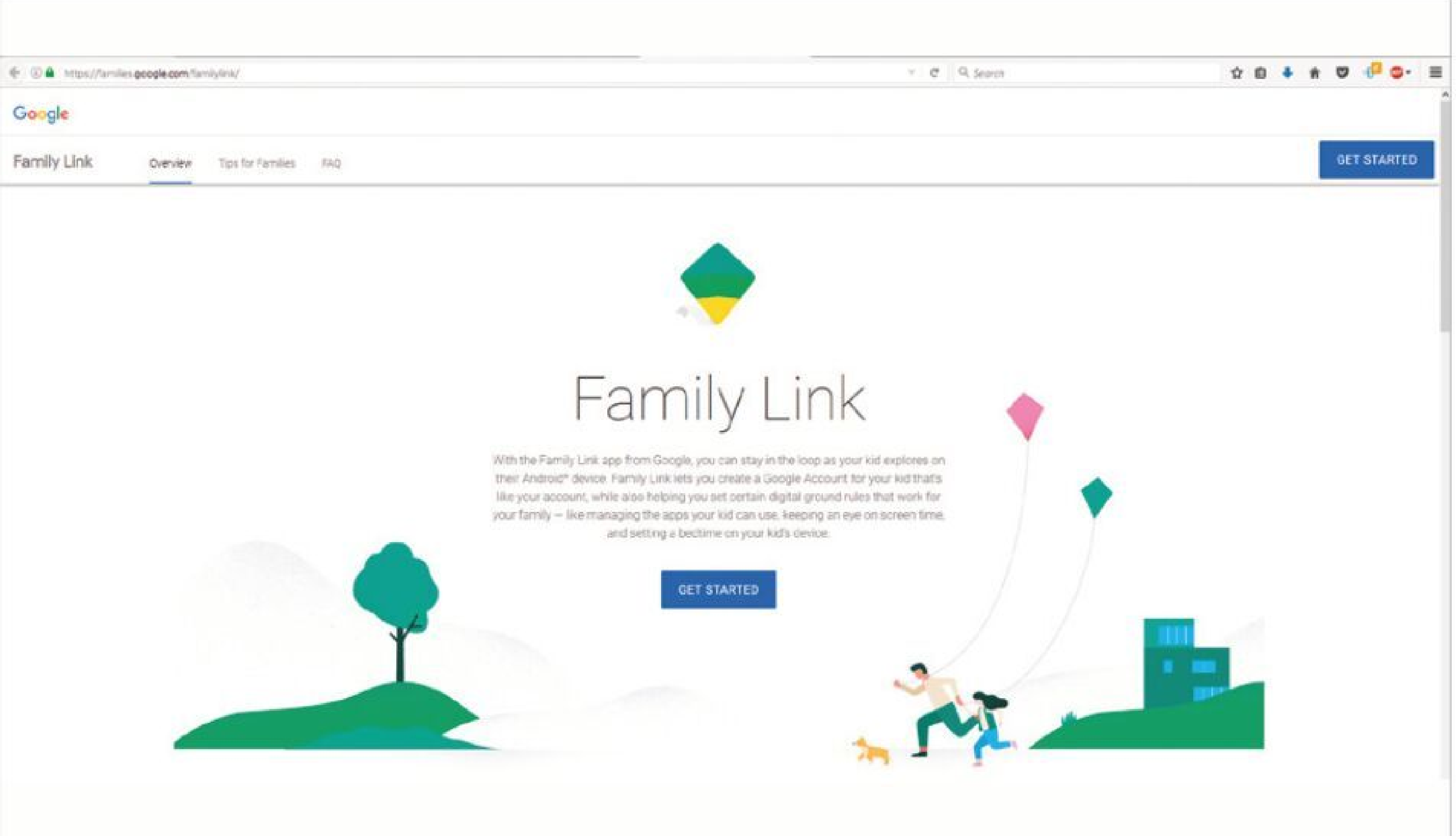
Secure, reliable email for your children.
Stop all spam, adverts and messages from anyone you don't know.
Use flexible parental controls to suit the needs of your whole family.
Try it today - completely free of charge.

GMAIL

Providing your child is thirteen years or older, they can get access to a Gmail account. Gmail isn't the first email service that springs to mind when considering a young person friendly email account but with careful use of its filters, you can set up a good and reasonably safe email environment for them.

FAMILY LINK

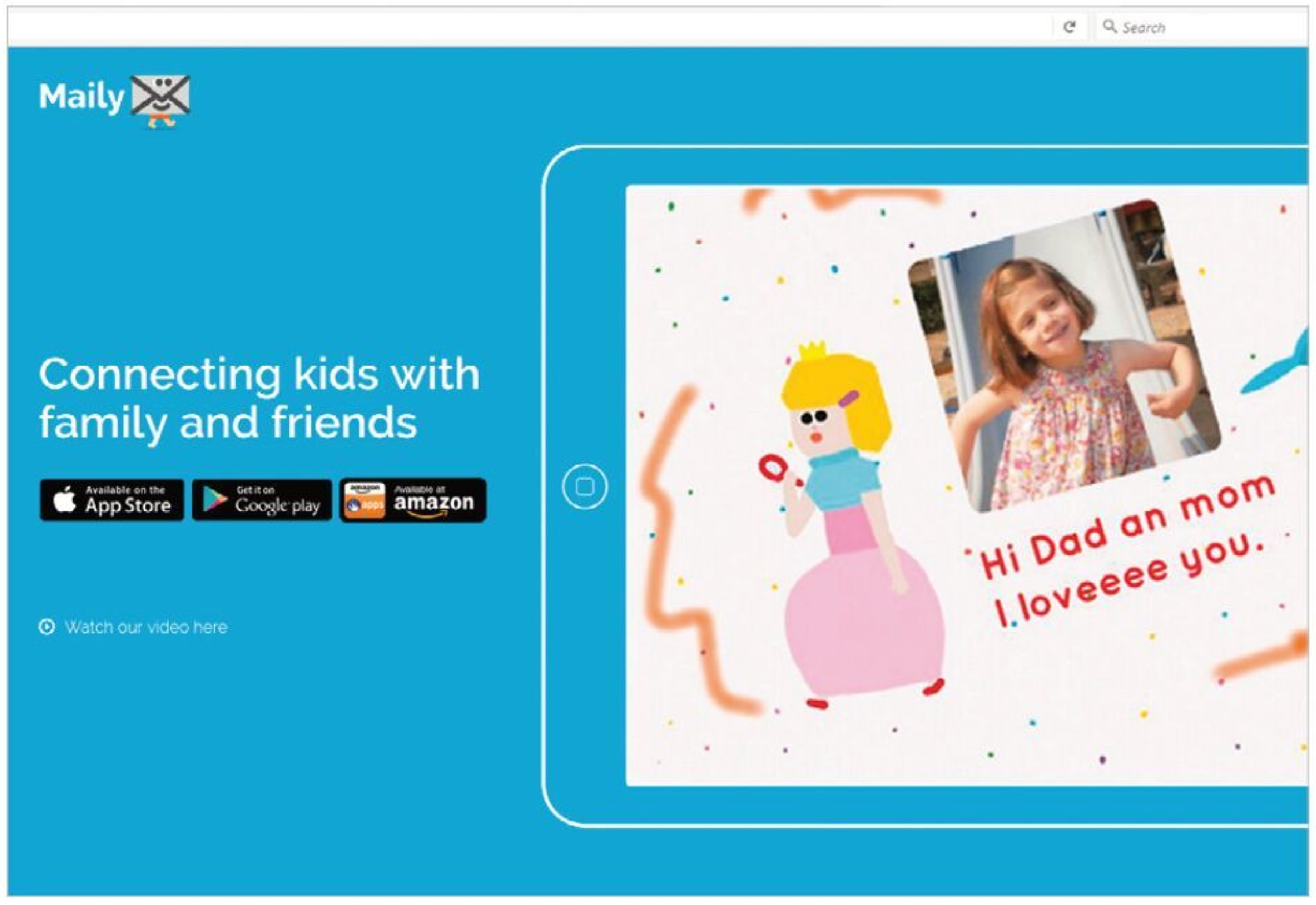
Part of the services offered by Google, Family Link can help you set up a Gmail-like account for children under the age of thirteen. You need to be located in the US for the moment but the service offers improved controls for Android devices and apps and there are considerations for moving the service outside of the US in time.


https://families.google.com/familylink/
Google
Family Link
Overview
Tips for Families
FAQ
GET STARTED
Family Link
GET STARTED

With the Family Link app from Google, you can stay in the loop as your kid explores on their Android* device. Family Link lets you create a Google Account for your kid that's like your account, while also helping you set certain digital ground rules that work for your family — like managing the apps your kid can use, keeping an eye on screen time, and setting a bedtime on your kid's device.

MAILY

This is a child-friendly email app for iOS and Android devices. It's fun to use, secure and offers the parent or guardian ample control and restrictions for the child's account. With it children can stay in contact with specified contact lists, whilst still remaining safe online.


Maily
Connecting kids with family and friends
App Store
Google play
amazon
Watch our video here
Hi Dad an mom I.loveeee you.

SCHOOL EMAIL

Here's an interesting suggestion, why not use the child's school email? Providing the school is willing to participate, a child can log into their account from home and using the elevated security, send and receive emails in total safety. Naturally, you'd need to confirm with the school prior to using the email for personal contact.

Cyberbullying

Cyberbullying is when someone uses the Internet, email, online gaming, social media and any other kind of digital platform to threaten, tease, humiliate or upset someone else. Both the bully and the victim of the bullying can be any age, from very young children up to late teens, and beyond in some cases. The source of the bullying can come from others the victim knows at school or college, or from a complete stranger on the other side of the world.

Bullying someone online doesn't always involve threating remarks. What may seem like a playful comment on one side, could be taken as a cutting jibe on the other. It's not always an easy thing to specify, as we all have moments when we may say or do something to upset someone without meaning to do that person any emotional harm. Mostly though, with respect to a loose and throw-away comment, the one who made the comment will probably apologise for their mistake once they realise that they have upset the other person.

However, true cyberbullying is the persistent harassment of an individual. The cyberbully will goad, threaten, send nasty messages, even take images of the victim and Photoshop them in inappropriate situations, through the use of many different forms of online communications.

It's a sad case too, that a lot of young people are already in a heightened emotional state due to their body image, thanks to the media and unrealistic Photoshopping of celebrities. Where young people, especially young teens, are very conscious of their image, a slight remark to someone can impact the young person in an incredibly negative way.

Social Media

Probably one of the main platforms for cyberbullying, social media is an ideal hunting ground for the cyberbully. The effects of social media bullying have been devastating on some families. Teen suicides, self harm and elevated cases of depression amongst young people are popular in the media and bring to light just how powerful and dangerous social media is as a communications tool.

Facebook, Twitter, Instagram and other examples have all become the haunt of those who prey upon and harass others. From the point of view of a child, whose emotional state is quite vulnerable, even a simple 'like' of a comment can embarrass or hurt.

Online Gaming

Another prime source of modern cyberbullying, online gaming has proved to be a vicious place to inhabit for some. The problem with online gaming is that the bullying comes from anywhere in the world. There are cases of gamers targeting females, different religions or those who come from different parts of the world. With the use of headsets, the gaming cyberbullies are able to shout threats and taunt other gamers, rallying others around them until the victims feel overwhelmed by bullies.

There are numerous games which have adopted a more sport-friendly approach, introducing policies whereby instances of bulling can be reported and the bullies themselves have their gaming accounts suspended. Often online gaming bullying is just someone shouting 'noob' at another, degrading the victim as a newcomer, or someone who isn't as good as them. Other times the bully will say things like 'I hope you die' or 'I'm coming to kill you', or something similar. In short, any abusive behaviour, including destroying your online game creations or belongings, is a form of bullying.

Text Messaging

With more and more young people having access to their own phones or tablets, abusive text messaging is becoming a major issue. Messages sent can, thankfully, be easily traced back to the source, and together with anyone else who was involved, the bully(s) can be reprimanded for their behaviour. Sadly though, there are ways to hide texts and with such knowledge, a cyberbully is able to send their abusive texts anonymously.

Another aspect of cyberbullying via text message is sexting. This is when someone takes an explicit image or video of themselves and sends it to someone else. Sometimes, a person can bully someone into sending them images or videos of the victim, then send those images on to others or upload them to popular sites and inform an entire group of their location.

Email

Sending abusive emails is a large area of concern for those involved in protecting young people from cyberbullying. We've seen, the double-edged blade of anonymity can cut both ways: it can protect your identity online but it also hide an individual who is bullying someone. Anonymous emails sent from a bully can be just as harmful as social media, online gaming and texting. It's a more personal form of bullying, much like having an abusive letter addressed and posted directly to you.

Setting up filters to block certain senders does work but only to a small degree. There are plenty of email services available that will hide a sender or fake email providers to hide behind. It's not always abusive content either, as cyberbullies have been known to send viruses and other malware via email to their victims.

Cyberbullying covers many different forms and platforms. It can be a single, throw-away comment, a like on a Facebook comment or just someone calling someone else a 'noob'. It can also be very serious indeed, including death threats, threats of violence or the sending or posting of explicit images or videos. There's a wealth of information available from the likes of the NSPCC and Childline with regards to cyberbullying, which is certainly worth reading through if you suspect any instances of bullying or you just want to know more about how it works online.

How to Prevent and Deal with **Cyberbullying**

We will never be able to truly stop cyberbullying, or any other form of bullying, from happening, as there will always be those who want to cause harm to others. However, we can take steps to prevent its effects, cope and deal with it.

Coping with face-to-face bullying can usually stop when the victim is home or at a place where they feel safe. On the other hand it often feels like there's no escape from cyberbullying as the online world is always present, and even when you cut yourself off from any online activities, the bullying still continues.

> “***Coping with Cyberbullying***”

The level of how upset a victim of cyberbullying feels depends greatly on the person. Some can easily shake it off or deal with it by immersing themselves in a sport, book, family or something else. Others though, take any form of abusive message, comment and such to heart and its affects can range from crying to feeling suicidal. There's a lot that goes on in between and it's difficult even for professionals and experts to say how to react and cope with cyberbullying.

However, there are some guidelines which we can help children and young people through when it comes to dealing with cyberbullying:

It's not your fault – If someone is repeatedly cruel to you, you must not blame yourself. Two people can have an argument but if the other person continually abuses you in some form, then that's bullying and is not acceptable.

Don't respond – No matter how easy or tempting it is to respond to a cyberbully, it's recommended that the young person doesn't. Often, a cyberbully is goading the victim for a response, it's a form of psychology that enables them to think they have power over the victim.

Save all evidence – It's important that the young person saves or records all the evidence of cyberbullying. This evidence can then be used to show a parent or guardian, teacher or relative, or even someone responsible for the platform where the bullying took place. This way action can be taken to prevent any escalation.

Always ask for help – Even if the bullying incident seems minor, such as a throw-away comment, it's always best for the young person involved to tell their parent or guardian. We, as adults, can then help the young person deal with the bullying.

Measure your response – It's very easy as a parent or guardian to make a knee-jerk reaction to someone who's cyberbullying our child. Therefore it's often best to take evidence, then perhaps contact someone else, such as the NSPCC or local councillor to see what they as professionals recommend as a gauged response.

Take time to listen – A young person coming to an adult for help on bullying is a huge step for them. It's easy to close up as a child, so to take that step should be worthy of your full attention. Listen to everything they have to say and together find a way to prevent and deal with the cyberbullies.

Help restore self-respect – The ultimate goal in any bullying is help restore self-respect to the victim. The more self-respect the young person has, then the better they are able to cope with future bullies, and life itself.

Stay positive – Bullying should be stopped but it's unlikely as humans will never be able to eradicate all forms of cruelty toward others. With that in mind, it's best to remain positive for the young person, whilst still being realistic. It will help them mature and learn to form protection techniques against those who want to cause suffering.

Ask the person to stop – Whilst one of the guidelines is to never respond, there is the option to take a simple approach and ask the person who's bullying to stop. Sometimes a hurtful comment could be easily rectified by the sender, simply by it being shown that it was unnecessarily cruel. In the ideal world, they will apologise and remove the comment. It depends greatly on the comment and bullying in question.

Use the tools available – Use the available filters, blocks and reporting mechanisms available to stop the cyberbully from even being able to contact you. Facebook, Twitter and so on can block users and you're able to report abusive behaviour. Likewise, online gaming can ban an account or kick a bully from the game server.

Report serious threats – Not only should you report threats to parents and guardians, it's recommended that you should report serious physical, sexual and violent threats to the police. Each case will be treated with respect and the police have powers to approach the bully with the evidence to caution or charge.

Whilst the above will help children, young people, parents and guardians with cyberbullying, it's sadly not something that's going to disappear overnight. The moment you're online, you're open to some form of abusive behaviour and every social media, online game and contact made increases the chances of cyberbullying from occurring. The best we can do is help young people cope with it and learn to avoid those who would want to abuse.

Helping Your Child Through the Internet

The Internet is a vast resource that's full of amazing details and an equal amount of villainy and inappropriate content. It's difficult for a child to navigate it by themselves and extremely dangerous; so, as a parent or guardian, we need to make sure they're safe.

Internet Safety for Everyone

Together with the excellent advice from the NSPCC, Childline and Safety Net Kids, we've collated ten practical and realistic tips to help you and your child remain safe when using the Internet and its connected services.

PERSONAL INFORMATION

Never post any personal information online. Keep your postal address, email address, phone numbers and, if possible, names away from public viewing. Especially never tell anyone you've just met online, in a game or chat room any details about yourself.

PERSONAL INFOR
Mr.
Mrs.
Ms.
First Name
Last Name

PHOTOGRAPHS

Consider carefully before posting any pictures of yourself online. Once an image is available on the Internet, it's extremely difficult to get rid of any trace of it; and should someone have already downloaded it on to their computer, it's impossible to locate and trace.

STRANGER DANGER

People you don't know in the real world are strangers and not always who they say they are. The same applies for the online world. Not everyone you meet in an online game is who they claim to be, so treat every contact as a stranger and be wary of them.

INAPPROPRIATE CONTENT

If you see or hear something online that upsets you or makes you feel uncomfortable, you must tell a parent, guardian or teacher as soon as you can. If possible, show them the content that's upset you and tell them why it's upsetting. Talking to a parent or teacher will help you gain a better understanding of the world around you.

COMMENTS

Always think before you enter any comments online. Remember, they can be hurtful to someone else or be inappropriate without you even realising it. The comments could also lead someone to taking an interest in you, if you enter your age for example.

ACCOMPANIED VIEWING

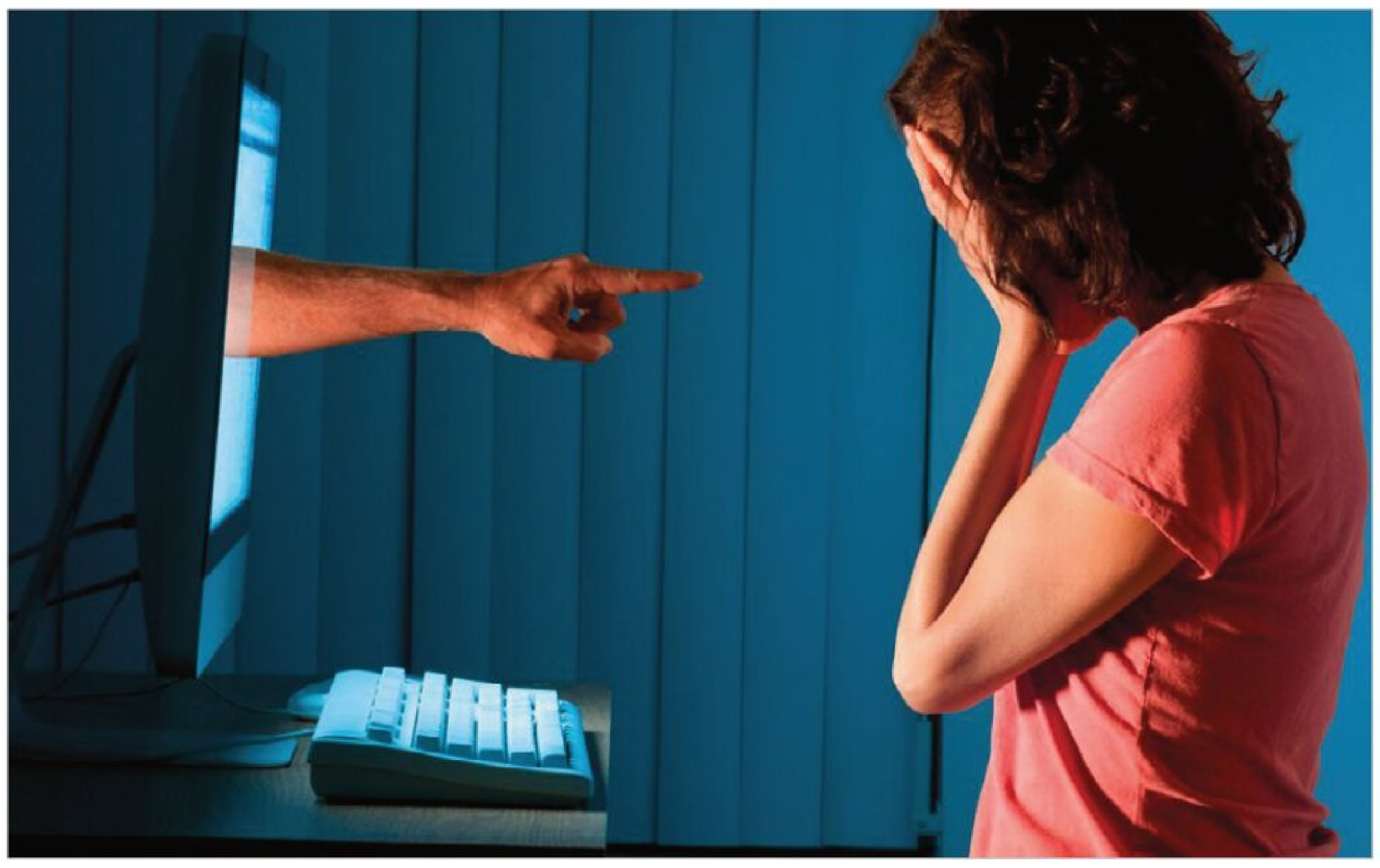
Parents, always make sure that young children are accompanied when navigating the Internet. Ensure that the privacy and security settings are as high as possible and that they don't have access to sites beyond what you specify, should you need to leave their side for a moment.

SECURE PASSWORD

Never give out your password online, even if the email or message is claiming to be from the bank or someone you know. Never let anyone remotely attach to your computer either. It's very rare for a company to attach to a home computer to fix something. At least be suspicious of anyone asking to connect remotely.

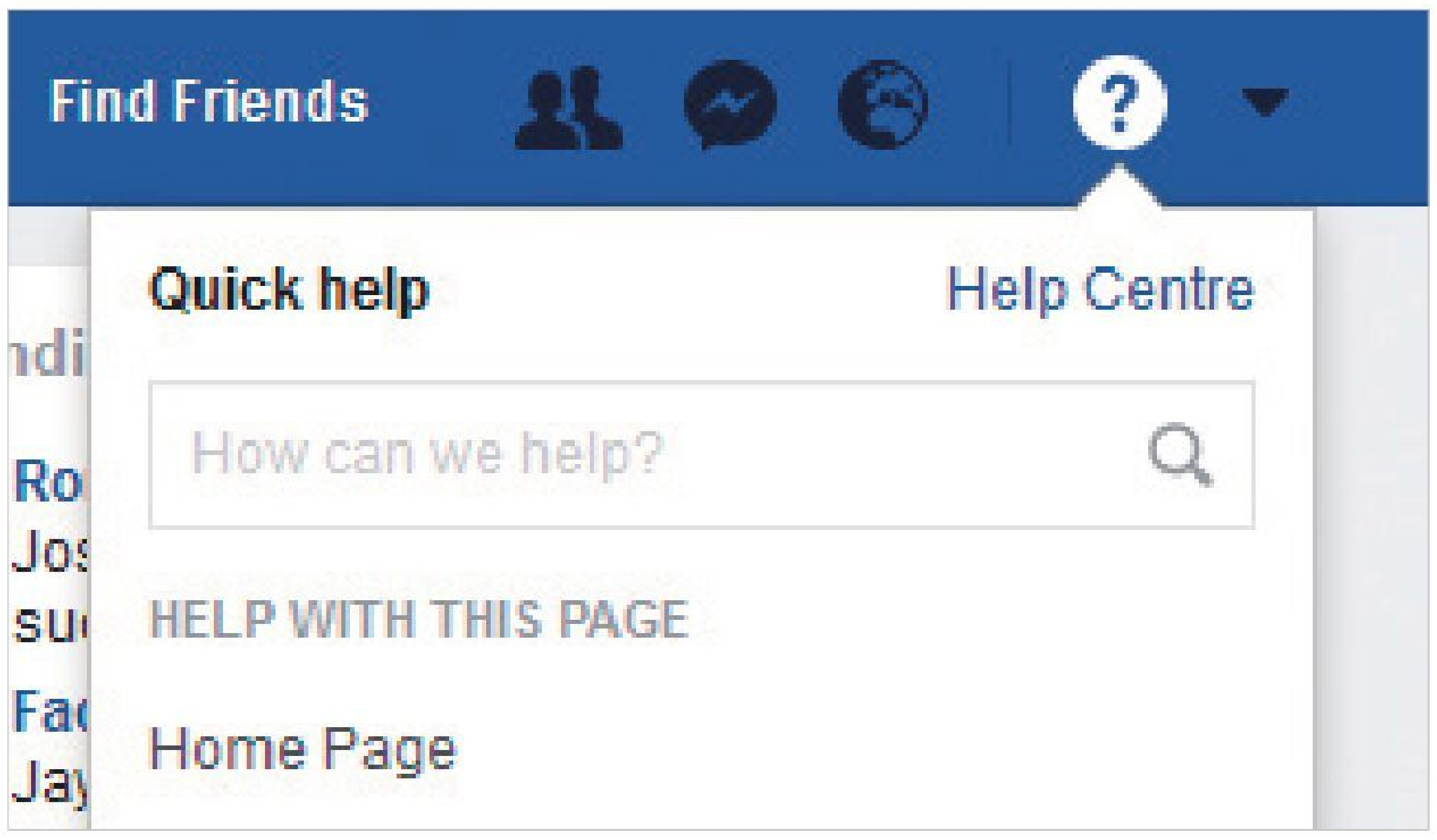
IGNORE BULLYING

Try not to reply to anyone who's appearing to bully you online. They are most likely trying to goad you into responding and will keep pushing until you finally crack and respond. Most of all, never respond out of anger. If it's getting too much, leave the site or game and come back later.



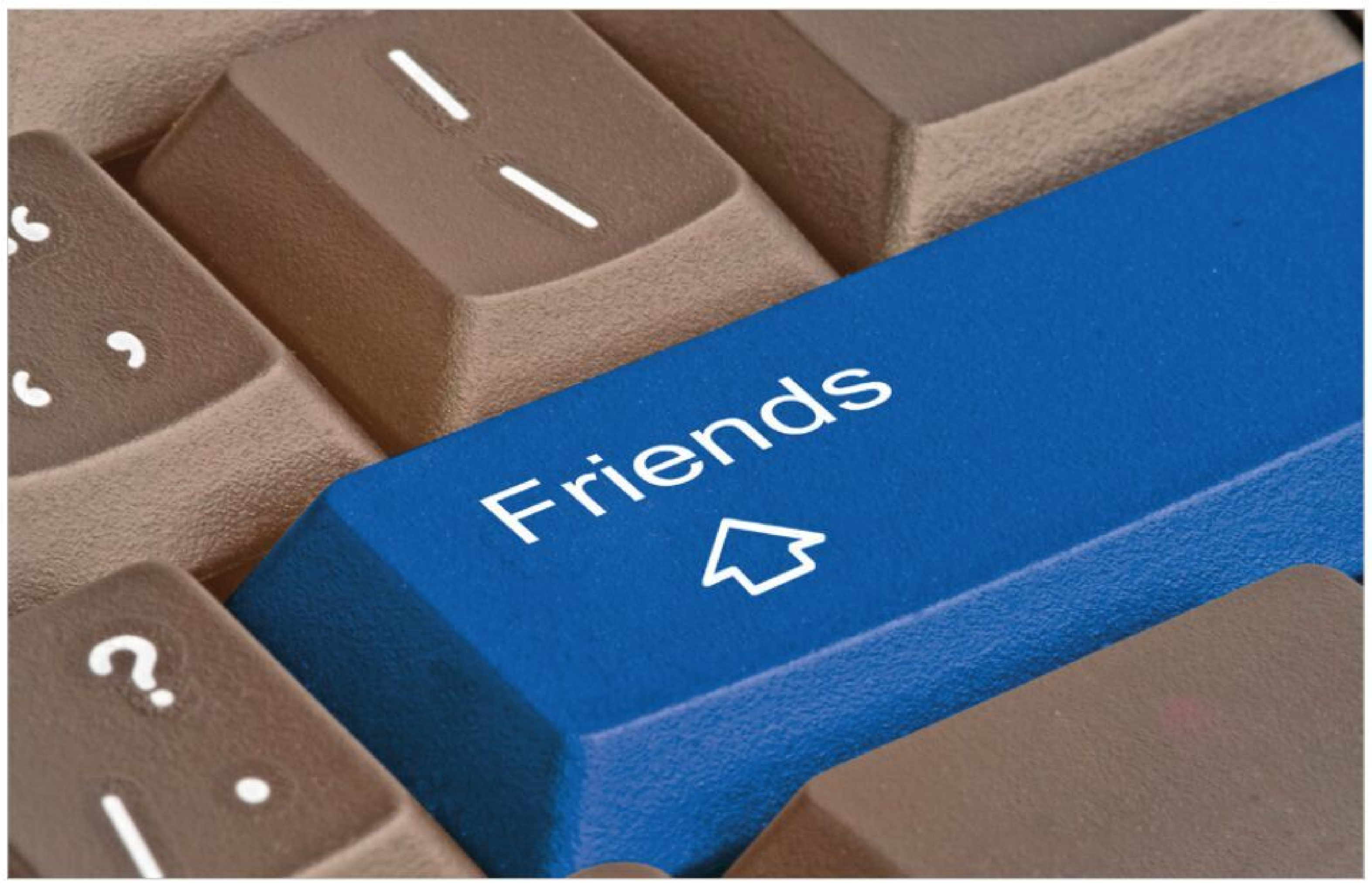
SOCIAL SAFETY

Whether you're on a social media site, in a chat room or playing a game, become familiar with the safety settings: how to turn off chat and how to block or report another user for any abusive content they may post. Take screenshots if possible, so you have evidence to back up your claim.



NEVER MEET

Never arrange to meet up with anyone you've met online, even if you're an older teenager. It's very easy to pretend to be someone, post a fake picture or take the identity of someone else. If you do arrange a meeting, make sure you're with other friends, in a public place and let others know where you are going.



Your Child and Online Gaming, is it Safe?

Gaming has taken some interesting leaps in technology since the days of feeding money into the arcade cabinets. However, with those advances comes a new level of online concerns for parents and guardians.

Of course, there's nothing wrong with gaming or online gaming. Despite the many years of people bemoaning that gaming is taking away something from a childhood, recent studies have actually shown that online gaming can increase social skills, help develop hand-to-eye coordination and, depending on the game, have educational benefits and help young people learn.

The problem is that not everyone always plays fair; some take great offence when they've been beaten by another player, resulting in the person beaten shouting or entering abusive comments. Other players use cheats to gain an advantage, making it near impossible for other players to even have a chance of winning or succeeding. Sometimes, when a player is better than others around them, they can be accused of cheating, even when they're not.

All of the above can be disheartening to a young person and depending on the amount and type of abuse they may receive from a poor loser, quite upsetting too. It's often difficult for someone who enjoys playing a particular game to be accused of something they haven't done or have to contend against someone who is obviously cheating. The trick of course is to keep calm, something many adults find difficult doing under such circumstances, let alone children and young people.

There are other factors too that can cause problems for young people when gaming. The game itself might not be age appropriate, with in-game missions asking the young person to do something that's really not very nice. The game might involve some scenes of an inappropriate nature, perhaps sexually explicit or extremely violent, or use inappropriate language.

In terms of online bullying, it's not just rage that causes problems. Griefing is a tactic used by some gamers to bully others into making the wrong move or decision in the game. This way, the 'griefer' wins by simply causing as much aggravation as possible, and in turn enrages those around them. It's also not unheard of for entire teams of griefers to band together to bully the opposition into defeat.

In-game spending is a modern cause for concern among parents too. For the young person who enjoys playing the game to have any significant advantage at all, they may need to purchase better items from the in-game store. Often these items will inevitably lead to more items needing purchasing and the cost soon mounts up. Other games make it near impossible to finish without having to pay for something, such as a key to unlock the next level or by having the player buy and download more content (known as a DLC, downloadable content).

The other safety concerns involve those who play games in order to be exposed to young gamers. Minecraft, for example, is a game predominantly played by younger people, so those of a perverse nature may play and use servers where they're interacting with younger people; there's even the possibility of some form of online grooming taking place in situations such as this.

However, despite the safety concerns over online gaming, it's not always bad news. Yes some games do employ tactics to leech more money from the players and other games are simply an excuse for poor behaviour; but with respect, there are countless games available that can help a young person develop social and other skills.

As parents and guardians, we need to make sure that the game the young person is playing is appropriate and, to some degree, useful to them, as well as being enjoyable. We'll look at some tips on staying safe when gaming online over the page but it's worth remembering that even if we find the game somewhat dull, the young person playing it may well be enjoying it. We just need to make sure it's a safe environment for them.

Online is playing a game in real time with other players from around the world. The game can be virtually anything, a shooter, role playing, adventure or something open world, such as Minecraft. The issue with online gaming is that anyone could be the character that's currently playing next to your child's online avatar.

> **Online Gaming**

Staying Safe when Gaming Online – Advice for Your Child

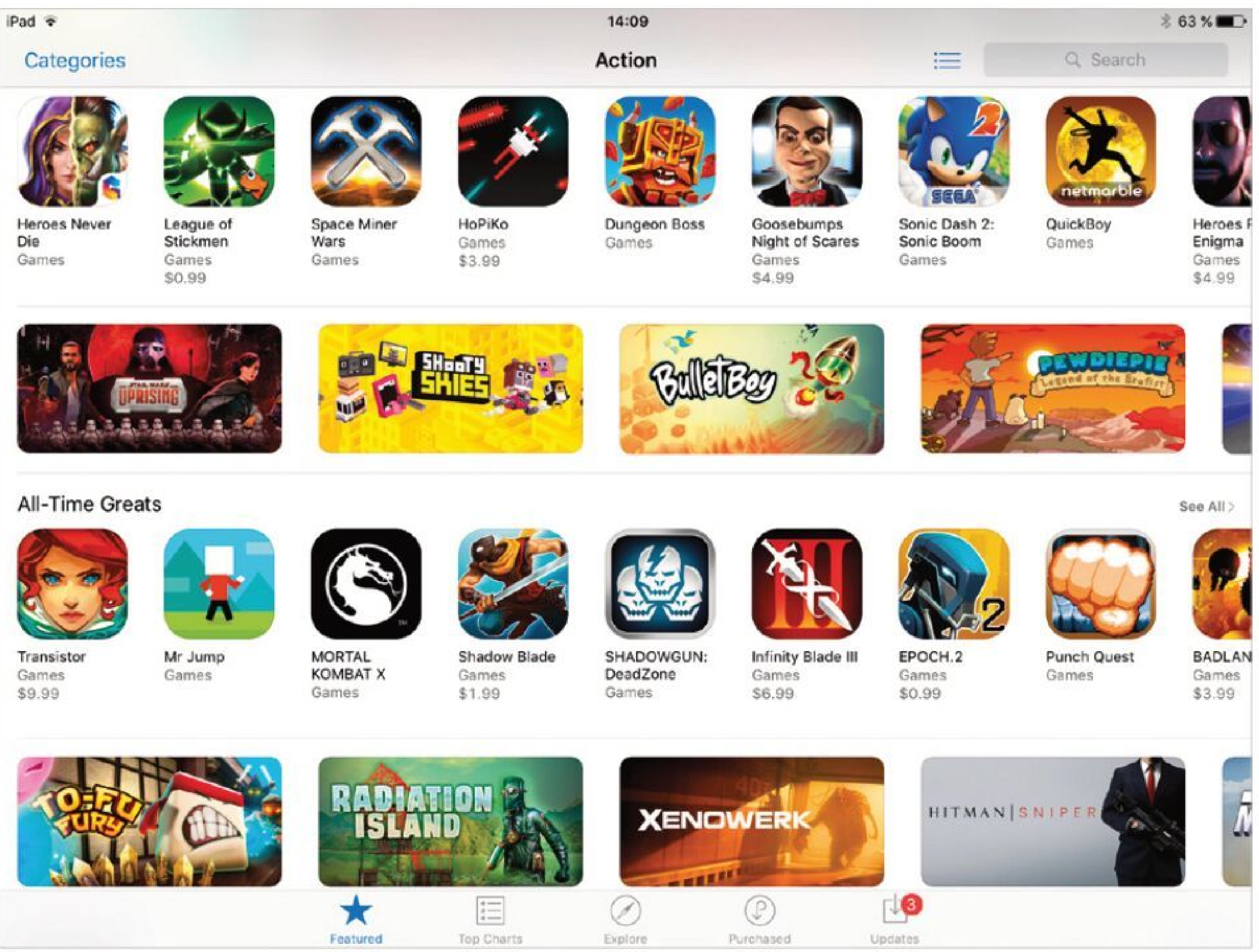
We've looked at the safety concerns of online gaming but what can we as parents and guardians do to help keep our young gamers safe? Thankfully, it's nothing too drastic, just a little common sense and a few tips to help out.

Game On

Here are ten tips to help the young gamer get the best from their game of choice, whilst still remaining safe; also how to avoid any conflicts that may arise from the gaming community.

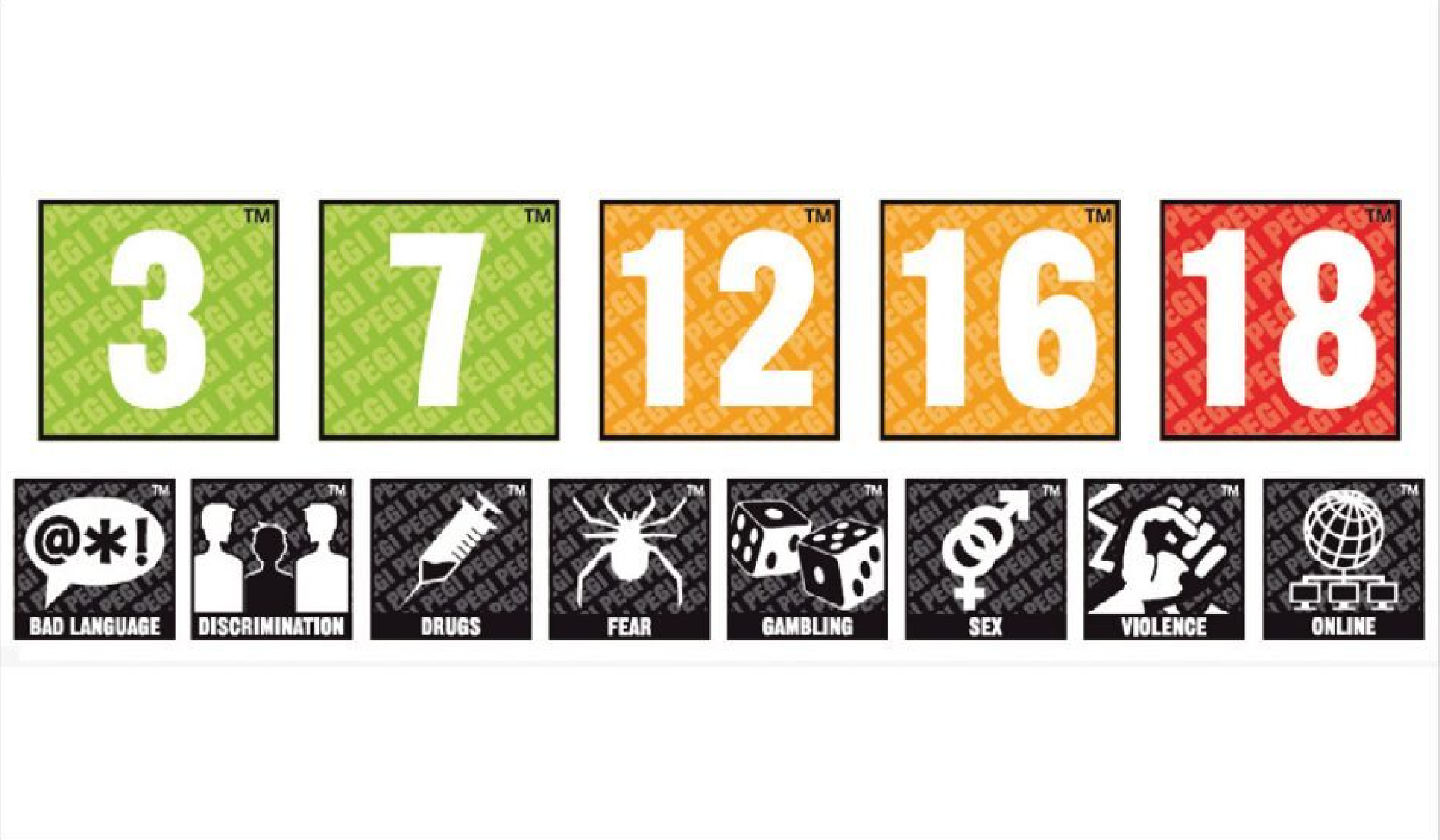
INVOLVED PARENTS

Parents, take an interest in the online games that your child plays. See what type of game it is and especially see what the online community is like. View the in-game chat, and read the game's forum if it has one to gauge the type of gamers who play it.


iPad
14:09
63 %
Categories
Action
Search
Heroes Never Die
League of Stickmen
Space Miner Wars
HoPiKo
Dungeon Boss
Goosebumps Night of Scares
Sonic Dash 2: Sonic Boom
QuickBoy
Heroes F Enigma
Shooty Skies
Bullet Boy
Pewdiepie Legend of the Brofist
All-Time Greats
See All
Transistor
Mr Jump
MORTAL KOMBAT X
Shadow Blade
SHADOWGUN: DeadZone
Infinity Blade III
EPOCH.2
Punch Quest
BADLAN
To-Fu Fury
Radiation Island
Xenowerk
Hitman Sniper
Featured
Top Charts
Explore
Purchased
Updates

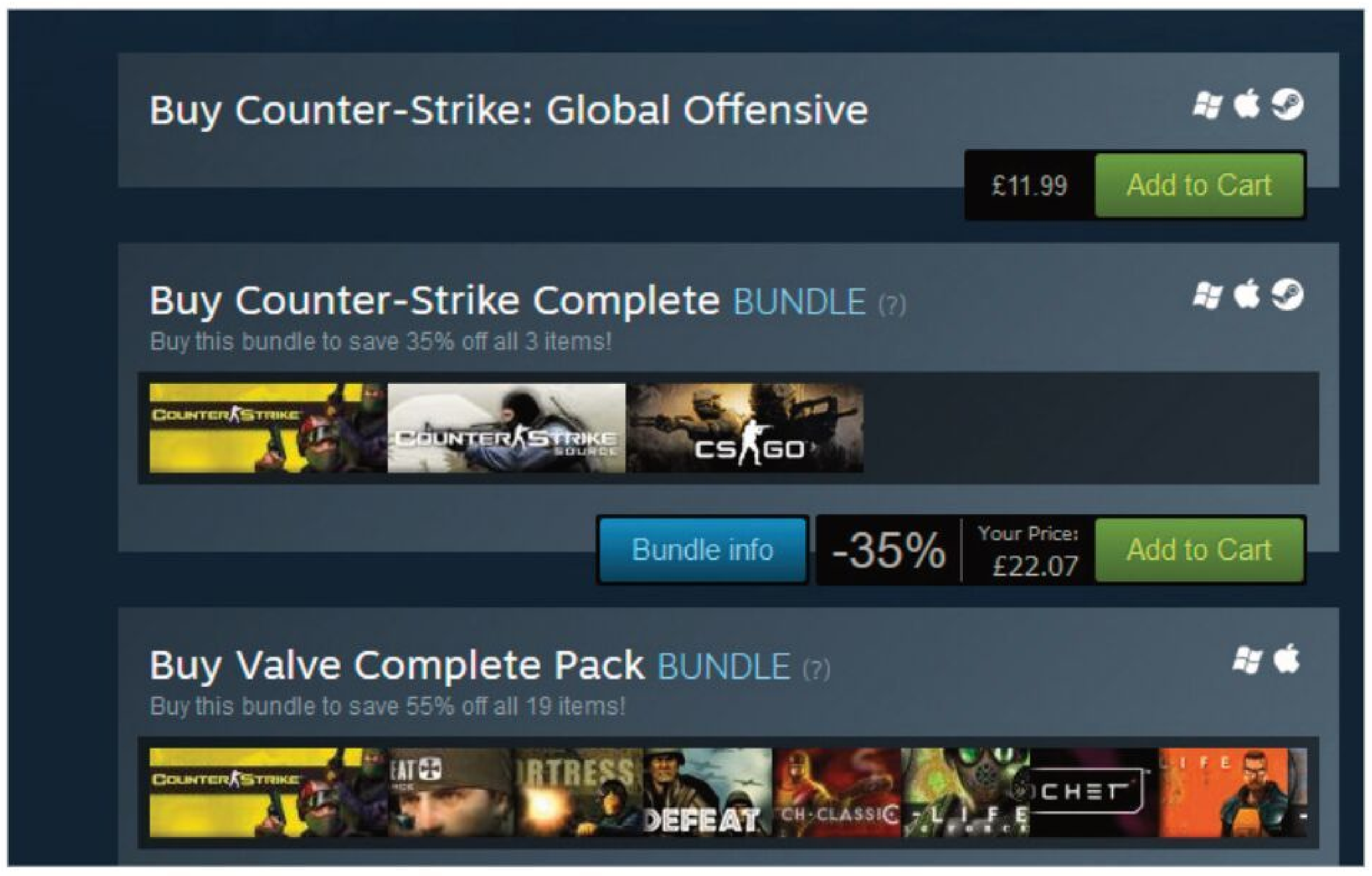
AGE APPROPRIATE

Make sure that game you're playing is age appropriate. Whilst it's fun being nine and playing an 18-rated game, there's bound to be content within that may upset or offend you. There's a reason certain types of game have an age restriction.


3
7
12
16
18
PEGI
BAD LANGUAGE
DISCRIMINATION
DRUGS
FEAR
GAMBLING
SEX
VIOLENCE
ONLINE

IN-GAME SPENDING

However tempting it is to buy an on-game item or DLC, it's not always the best idea. Items like this can be a lure for you to buy another and another, until the cost mounts up and you've racked up a game bill in the hundreds. If you desperately need an item, discuss it with a parent or guardian.



Buy Counter-Strike: Global Offensive

£11.99 Add to Cart

Buy Counter-Strike Complete BUNDLE (?)

Buy this bundle to save 35% off all 3 items!

Bundle info -35% Your Price: £22.07 Add to Cart

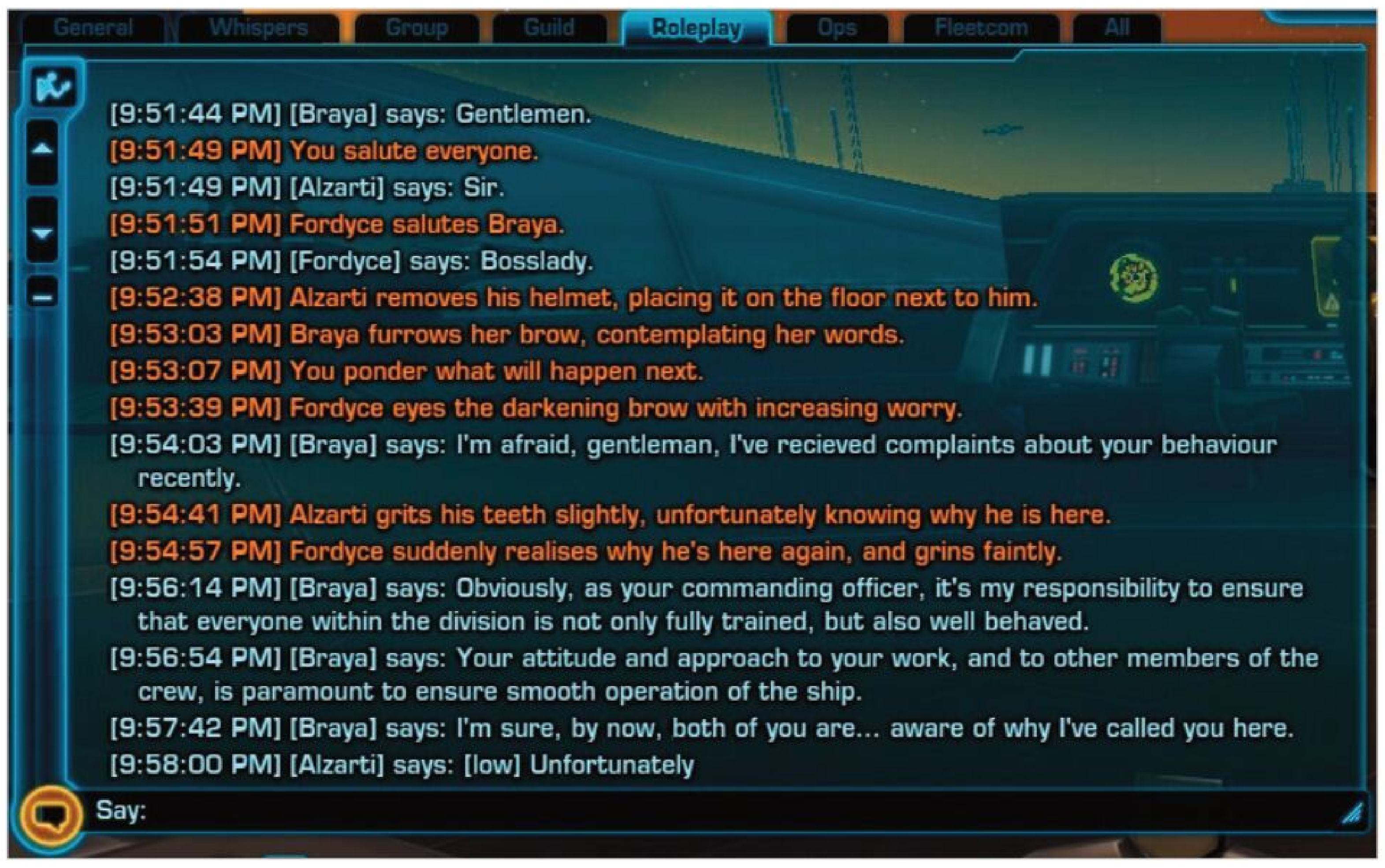
Buy Valve Complete Pack BUNDLE (?)

Buy this bundle to save 55% off all 19 items!

COUNTER-STRIKE
COUNTER-STRIKE SOURCE
CS:GO
DEFEAT
HALF-LIFE

CAREFUL CHATTING

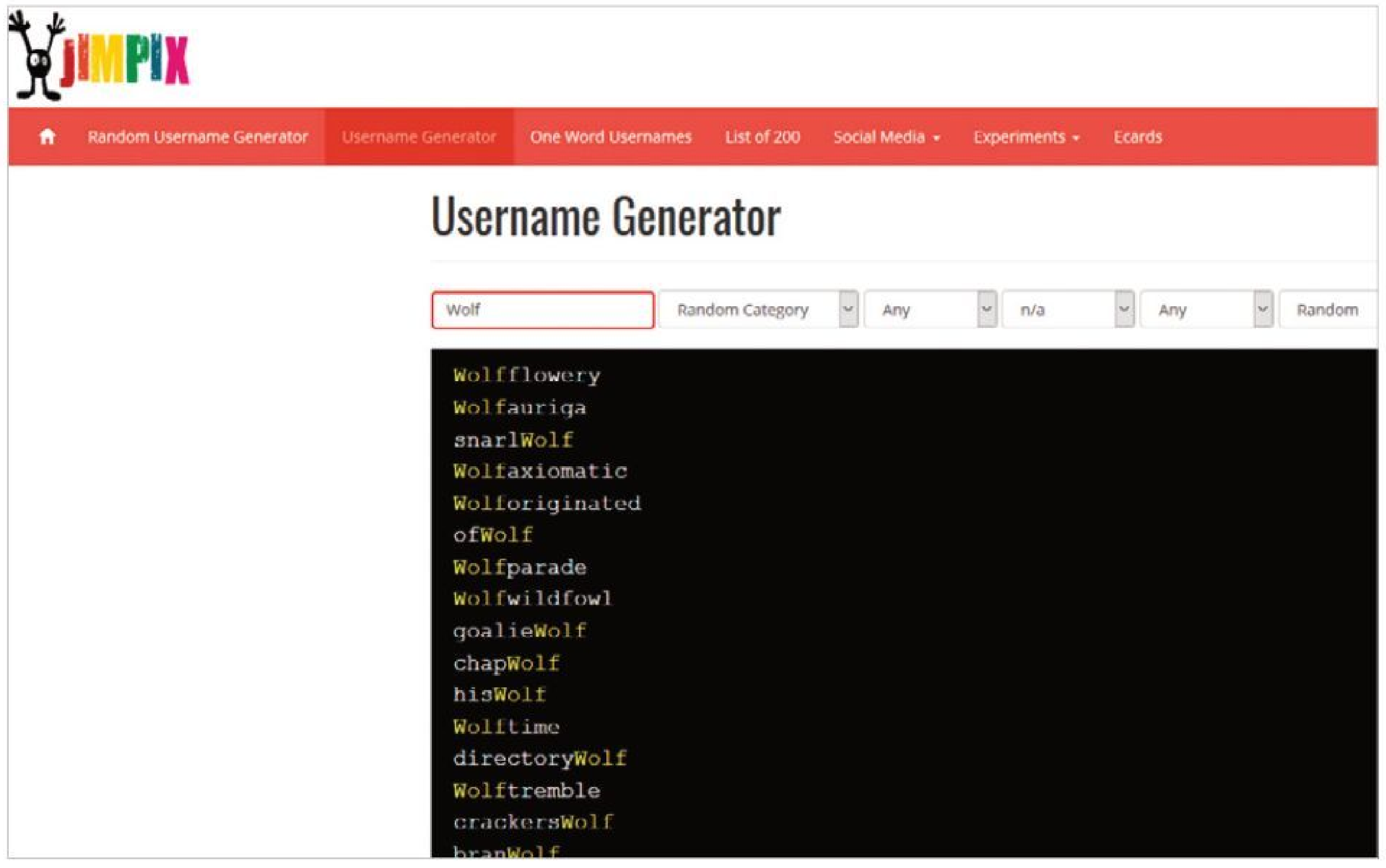
Not everyone in the game is going to be the same age as you. There are some people who are much older and who like to pretend they're a young person. Don't be fooled into becoming a friend with someone who's playing with you. Enjoy the game, and playing with others, but don't arrange any out of game communications.


General
Whispers
Group
Guild
Roleplay
Ops
Fleetcom
All

```
[9:51:44 PM] [Braya] says: Gentlemen.
[9:51:49 PM] You salute everyone.
[9:51:49 PM] [Alzarti] says: Sir.
[9:51:51 PM] Fordyce salutes Braya.
[9:51:54 PM] [Fordyce] says: Bosslady.
[9:52:38 PM] Alzarti removes his helmet, placing it on the floor next to him.
[9:53:03 PM] Braya furrows her brow, contemplating her words.
[9:53:07 PM] You ponder what will happen next.
[9:53:39 PM] Fordyce eyes the darkening brow with increasing worry.
[9:54:03 PM] [Braya] says: I'm afraid, gentleman, I've recieved complaints about your behaviour
  recently.
[9:54:41 PM] Alzarti grits his teeth slightly, unfortunately knowing why he is here.
[9:54:57 PM] Fordyce suddenly realises why he's here again, and grins faintly.
[9:56:14 PM] [Braya] says: Obviously, as your commanding officer, it's my responsibility to ensure
  that everyone within the division is not only fully trained, but also well behaved.
[9:56:54 PM] [Braya] says: Your attitude and approach to your work, and to other members of the
  crew, is paramount to ensure smooth operation of the ship.
[9:57:42 PM] [Braya] says: I'm sure, by now, both of you are... aware of why I've called you here.
[9:58:00 PM] [Alzarti] says: [low] Unfortunately
Say:
```

NOTHING PERSONAL

Never give out any personal details into an in-game chat window, via your headset or in a game's forum. These places are ideal hunting grounds for those who want to use that information to their advantage. Make sure your username isn't linked to you in real life too.


jIMPIX
Random Username Generator
Username Generator
One Word Usernames
List of 200
Social Media
Experiments
Ecards
Random Category
Any
n/a
Any
Random

Username Generator

Wolf

Wolfflowery
Wolfauriga
snarlWolf
Wolfaxiomatic
Wolforiginated
ofWolf
Wolfparade
Wolfwildfowl
goalieWolf
chapWolf
hisWolf
Wolftime
directoryWolf
Wolftremble
crackersWolf
branWolf

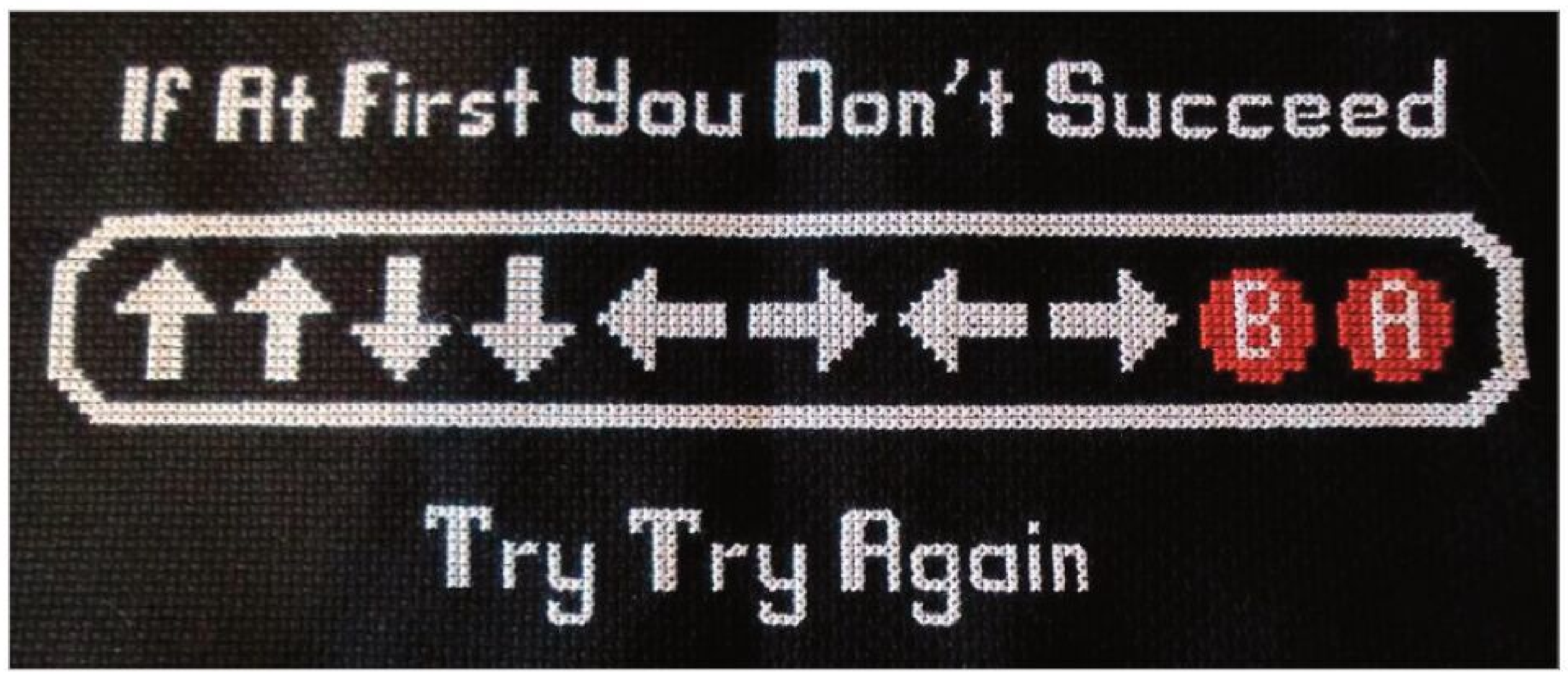
NO GRIEVING

Try not to get angry or be fooled by someone who's being nasty in the game. They could be baiting you, griefing you into making a mistake or simply just a cyberbully who's looking for someone new to inflict misery on. Don't react to anyone calling you a noob, loser or any such wording.

STOP GRIEFING!

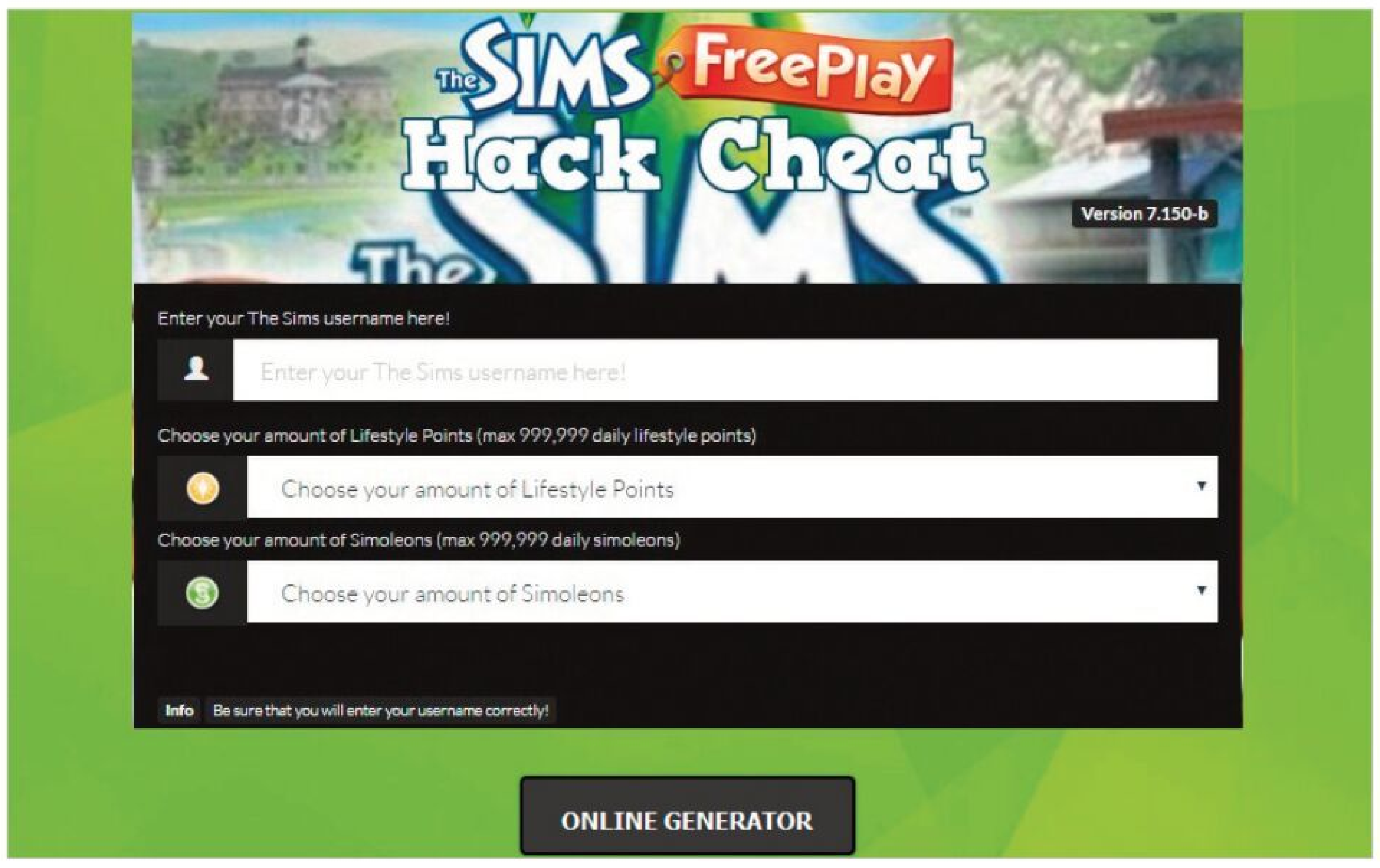
AVOID CHEATING

Cheats are everywhere. Even in the most secure game, there will be a time when someone releases a cheat code that can grant them immortality, infinite items or something else that enables them to win all the time. If you can, record their activity and report them to the game server admins.


If At First You Don't Succeed
↑↑↓↓←→←→ B A
Try Try Again

AVOID HACKING

Don't attempt to download or sign up for a site that claims to give you an in-game advantage or cheat. Some downloads and sites contain malware payloads or are trying to scam you in some way. Whilst it's tempting to have the advantage, it's nearly always some form of phishing scam.


The SIMS FreePlay Hack Cheat
Version 7.150-b
ONLINE GENERATOR

Enter your The Sims username here!

Enter your The Sims username here!

Choose your amount of Lifestyle Points (max 999,999 daily lifestyle points)

Choose your amount of Lifestyle Points

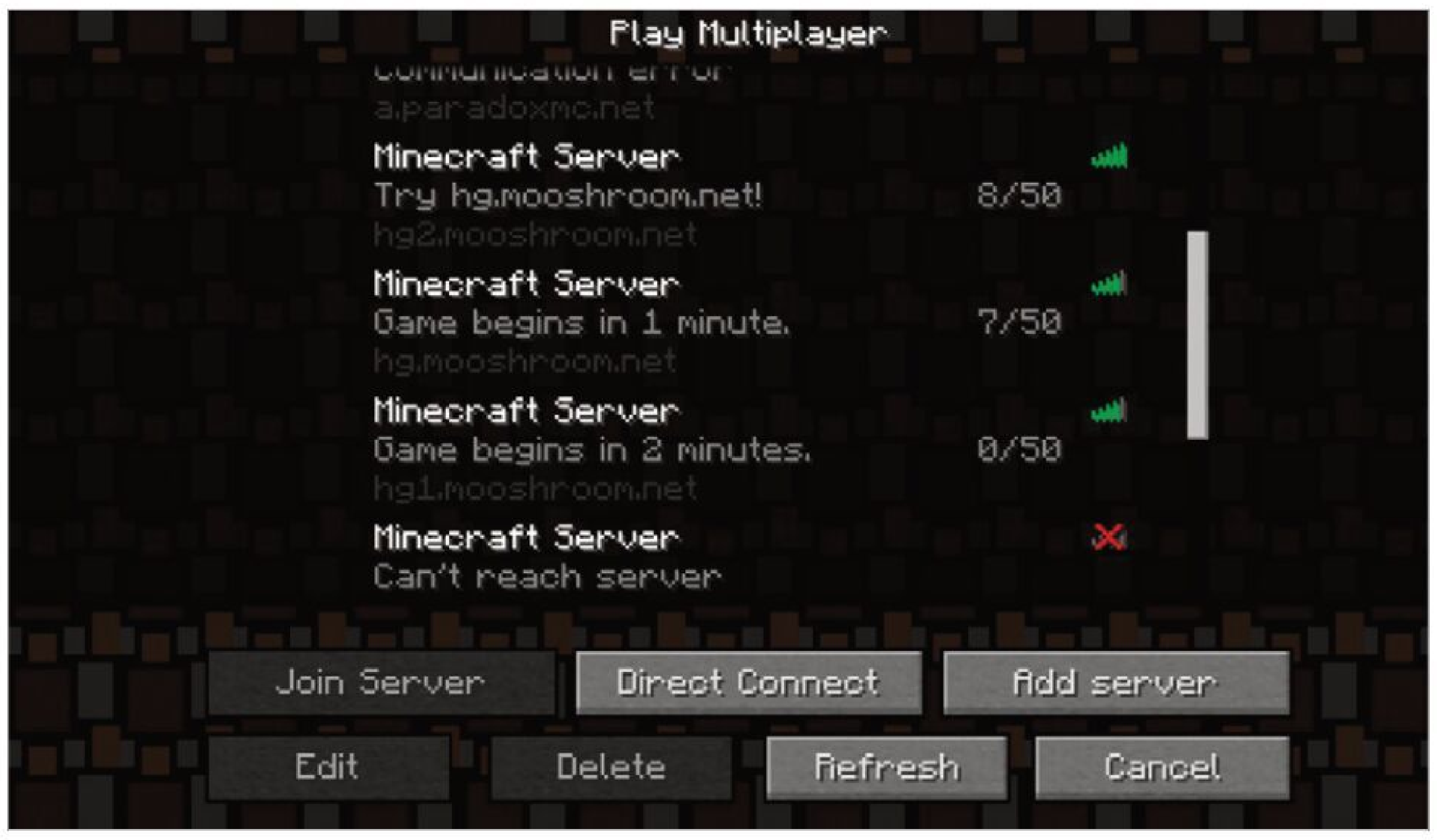
Choose your amount of Simoleons (max 999,999 daily simoleons)

Choose your amount of Simoleons

Info Be sure that you will enter your username correctly!

ALTERNATIVE SERVERS

If you find yourself on a server with cheats, the subject of griefing or other forms of bullying, then leave the server and see if there's another one available without these people present. It might also just be a bad time of day, so try again later on.


Play Multiplayer
Join Server
Direct Connect
Add server
Edit
Delete
Refresh
Cancel

a.paradoxmc.net

Minecraft Server
Try hg.mooshroom.net! 8/50
hg2.mooshroom.net

Minecraft Server
Game begins in 1 minute. 7/50
hg.mooshroom.net

Minecraft Server
Game begins in 2 minutes. 0/50
hg1.mooshroom.net

Minecraft Server
Can't reach server

WARY TRADING

Be wary of any in-game comments offering a discount on in-game items or trades. Whilst some are legitimate, people wanting to trade one item for another, others are trying to scam you out of real money or in-game cash or items.

MATCHMAKING: SOLO
SATURN
URANUS
NEPTUNE
PLUTO
CERES
ERIS
SEDNA
EUROPA
PHOBOS
DERELICT
MERCURY
ance
Recruiting
Trading
HOLD RIGHT CLICK TO ROTATE

TS > Sancti Tigris offer
WTS - Narrow Minded / Constitution/ Hell
Storm/Ravage/Focus Energy/WildFire/ Toxic
eed / Corrupt Charge / Rending Strike / Bite /
g Prime Set ! Good price , pm me if want
ugh: Selling Loki Prime Helmet
c WTB>vaykor hek and sancti tigris offer me
S>Volt prime Chassis 60P, Maxed Serration
asia tradign
ite for 100plats
>Prisma Tetra, Bo p set
asia trading
TS > Frost Bite

-DarkTenno-
-V-E-G-A-
21stgun-EN-
_AzE_BoSS_
Rue
yogoy
AHRI3
ALIAS2050
ArchonLegend

Monitoring What's Going On

The temptation and lure of the Internet is often a little too much for some people, especially young people who are repeatedly told not to look or go somewhere on it. Tell a young person not to open a box and most will lift the lid when you're not around.

The tech-savvy youngsters of today will already have a better idea of how to circumvent technological restrictions that we've put in place. We're not saying they're hacking or do anything particularly bad, it's just that sometimes we need to see what all the fuss is about ourselves, rather than take someone else's word for it. Here then, are some of the tricks that the modern, digitally capable young person can do to hide what they look at on the Internet.

Private Browsing

Private browsing, privacy mode or incognito mode is a feature built into every browser, regardless of the computer or device's operating system. It is, as the title suggests, a privacy feature that will disable the browsing history and web cache; it stops any data from the browsing activities from being stored on the device or computer.

With private browsing mode enabled, which takes just a couple of clicks of the mouse, someone can effectively run a search for something they shouldn't, view the content and close down the private browser window without anyone ever knowing they were on the site. There are ways and means in which you can check for private browsing but it's often hit and miss and not entirely accurate, which is the whole point of private browsing in the first place.

Webmail

It's easy enough for someone to create a webmail account, such as Yahoo or Gmail and use it without anyone knowing of its existence. Combine a webmail account with private browsing, for example, and a young person could have an entirely anonymous email account without there being any trace of it on your system, as nothing will be stored locally.

There are also plenty of fake email services available, so in effect a different persona could be created with relative ease, as we've seen in previous anonymous and privacy sections of this book. Either way, it's certainly possible for a young person to have an email account you know nothing about.

Burner Phones

Whilst a burner phone is usually a phrase we hear on TV cop shows, the reality is startlingly close. It's not unheard of for a young person, often a teen with a job, to purchase a second pay-as-you-go phone that they can use to contact someone or access the Internet and other apps without you knowing.

Never underestimate the resourcefulness of a young person. Just as with a cop show burner phone, it's an easy

enough device to hide from a parent or guardian. Naturally there's a limit to what a young person can get away with but it's something worth keeping in mind. Another of the many elements to look out for with a young person who's being groomed, is a burner phone the groomer may give to them. This way, they're able to contact the young person with a higher degree of anonymity.

Secret Social Media

When used with an unknown webmail address, and private browsing, it's an easy task to create a secret social media account. Try it yourself and see how far you can get using Twitter and Facebook and the like.

Despite the fact that creating a fake social media account is against the social media platform's rules, it's not something they're able to police with any great efficiency. Just like a secret email, it's extremely difficult to see if a young person has set up a secret social media account.

OS on a stick

It's possible to have an entire operating system on a USB stick and be able to boot into the OS outside the system that's installed on the computer. This makes for an impressively anonymous and secure platform to browse from, as everything is done via the USB stick and the temporary session held in memory.

Naturally, the young person will need to reboot the computer and boot into the OS on the USB drive but that takes mere seconds these days. The end result is something you'll never likely be aware of.

Of course, we're not saying you should police your children like a prison warden. There will come a point where you simply have to have faith that you've taught them right from wrong and let them go and discover the world by themselves, however painful that may be. There's a fine line between protection and controlling and its borders are ever shifting thanks to the technology available and the ever-growing curiosity of young people.

However, we can make sure that a young person is educated and Internet-wise enough to be able to make decisions for themselves; and, as you would expect, we also need to ensure that they're not the victim of any digital attack. An open relationship is credited as being the key here, as often stated by professional bodies.

Human nature finds most of us sneaking a peek at something we shouldn't and children and young people are certainly no different. Young children will most likely avoid those areas on the Internet the parent or guardian has told them to never go to; however, older children and teens may find it a little too tempting.

> “*Eyes in the Back of Your Head*”

Monitoring Online Activity for Non-Technical Guardians

There's a vast difference between monitoring a child's online activity and actively spying on everything they do. In monitoring, you're making sure that they aren't being scammed, downloading anything illegal and generally behaving themselves online.

Non-Technical Tips for Monitoring

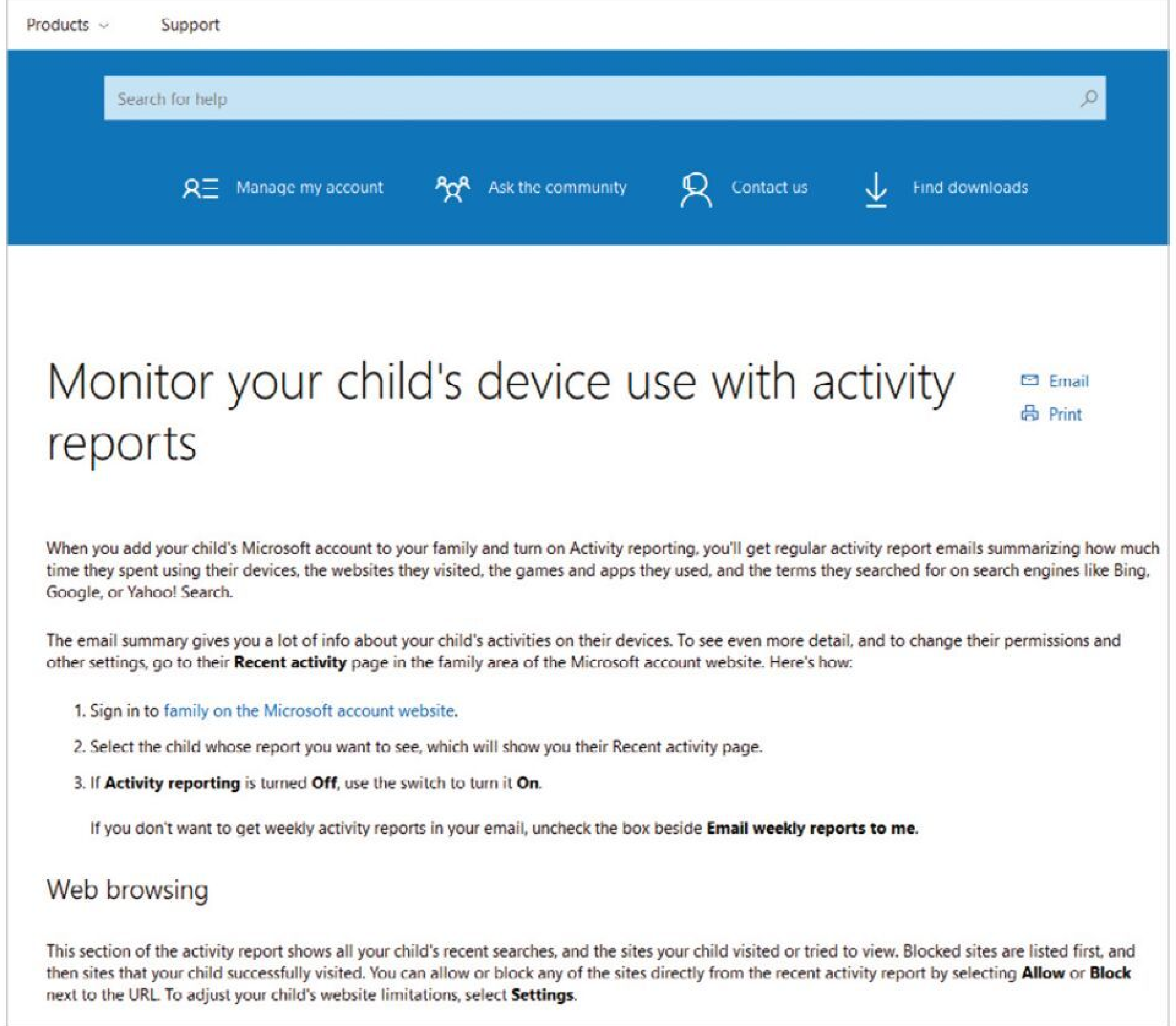
There are numerous ways to monitor a child's online safety but a lot of them can be quite technical. Instead, here are ten tips for those who aren't as computer literate but still want to help keep a child safe online.

DEFINE RULES

First off, set some rules. Don't use the Internet alone in your room, don't chat with anyone online, don't enter your full name or address online, don't click on any links, don't open any attachments, and talk if you see something that's upsetting. Common sense rules will go a long way to ensuring online safety.

FAMILY ACCOUNTS

Consider using the Microsoft Family Account as your child's login to Windows 10. We'll go into more detail as how to set it up and use it a bit later on. For now though, navigate to **https://support.microsoft.com/en-us/help/12441/microsoft-account-monitor-child-device-activity** and see what you can do with a child account in Windows 10.



Monitor your child's device use with activity reports

When you add your child's Microsoft account to your family and turn on Activity reporting, you'll get regular activity report emails summarizing how much time they spent using their devices, the websites they visited, the games and apps they used, and the terms they searched for on search engines like Bing, Google, or Yahoo! Search.

The email summary gives you a lot of info about your child's activities on their devices. To see even more detail, and to change their permissions and other settings, go to their **Recent activity** page in the family area of the Microsoft account website. Here's how:

1. Sign in to family on the Microsoft account website.
2. Select the child whose report you want to see, which will show you their Recent activity page.
3. If **Activity reporting** is turned **Off**, use the switch to turn it **On**.

If you don't want to get weekly activity reports in your email, uncheck the box beside **Email weekly reports to me**.

Web browsing

This section of the activity report shows all your child's recent searches, and the sites your child visited or tried to view. Blocked sites are listed first, and then sites that your child successfully visited. You can allow or block any of the sites directly from the recent activity report by selecting **Allow** or **Block** next to the URL. To adjust your child's website limitations, select **Settings**.

ISP HELP

If you require some extra help with monitoring the Internet activity in your home, consider contacting your ISP and chatting with a member of the team. Most, if not all, ISPs will have a dedicated section for online safety, in particular child safety and may be able to set up a web-based monitoring portal for you.

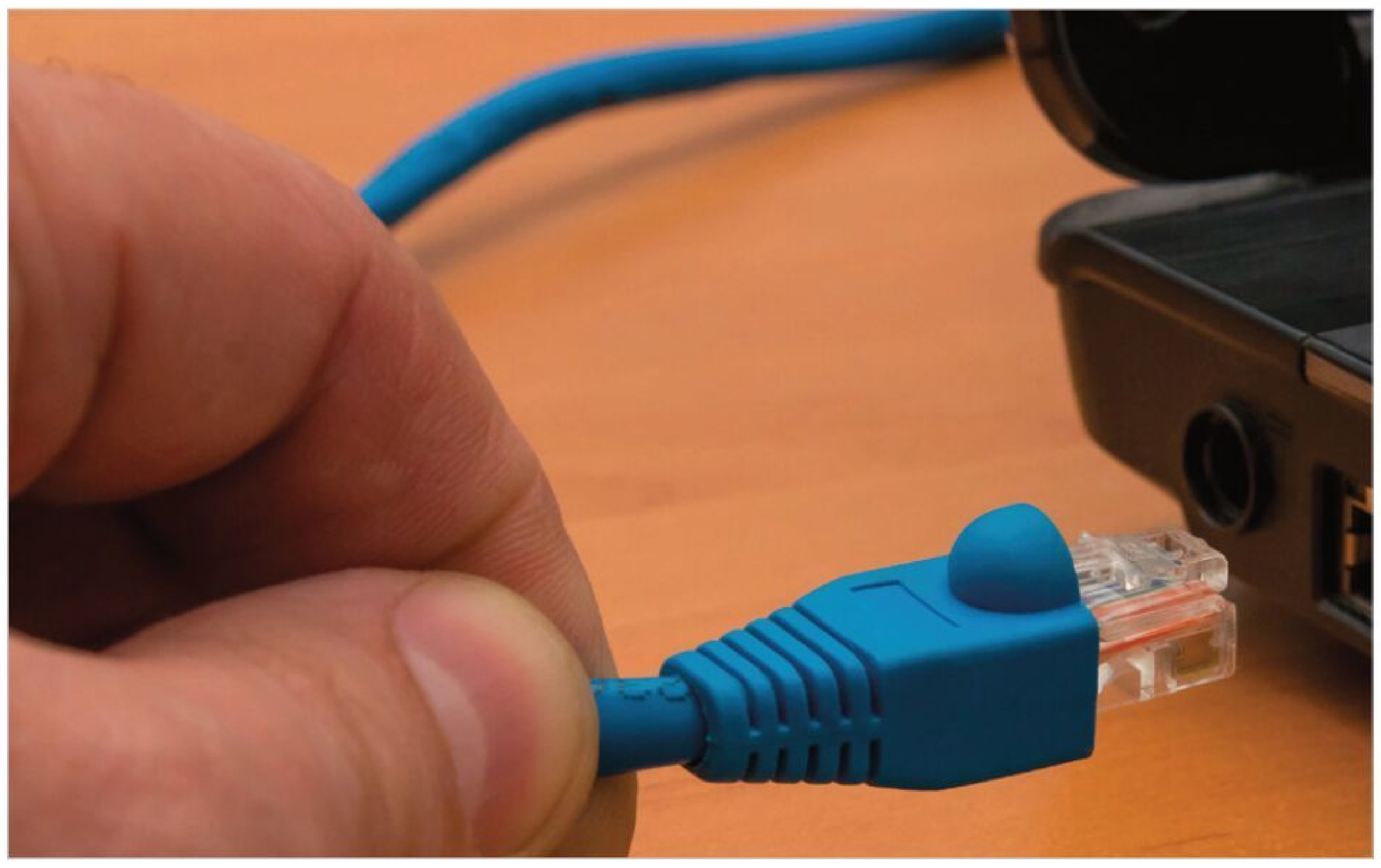
ISP
Internet Service Provider

BE PRESENT

Even if there are multiple computers and devices in the home, only allow the child to use one located in a main living area, such as the living room. Somewhere you're likely to be when they're online, so you can keep an eye on them and be at hand if they come across anything.

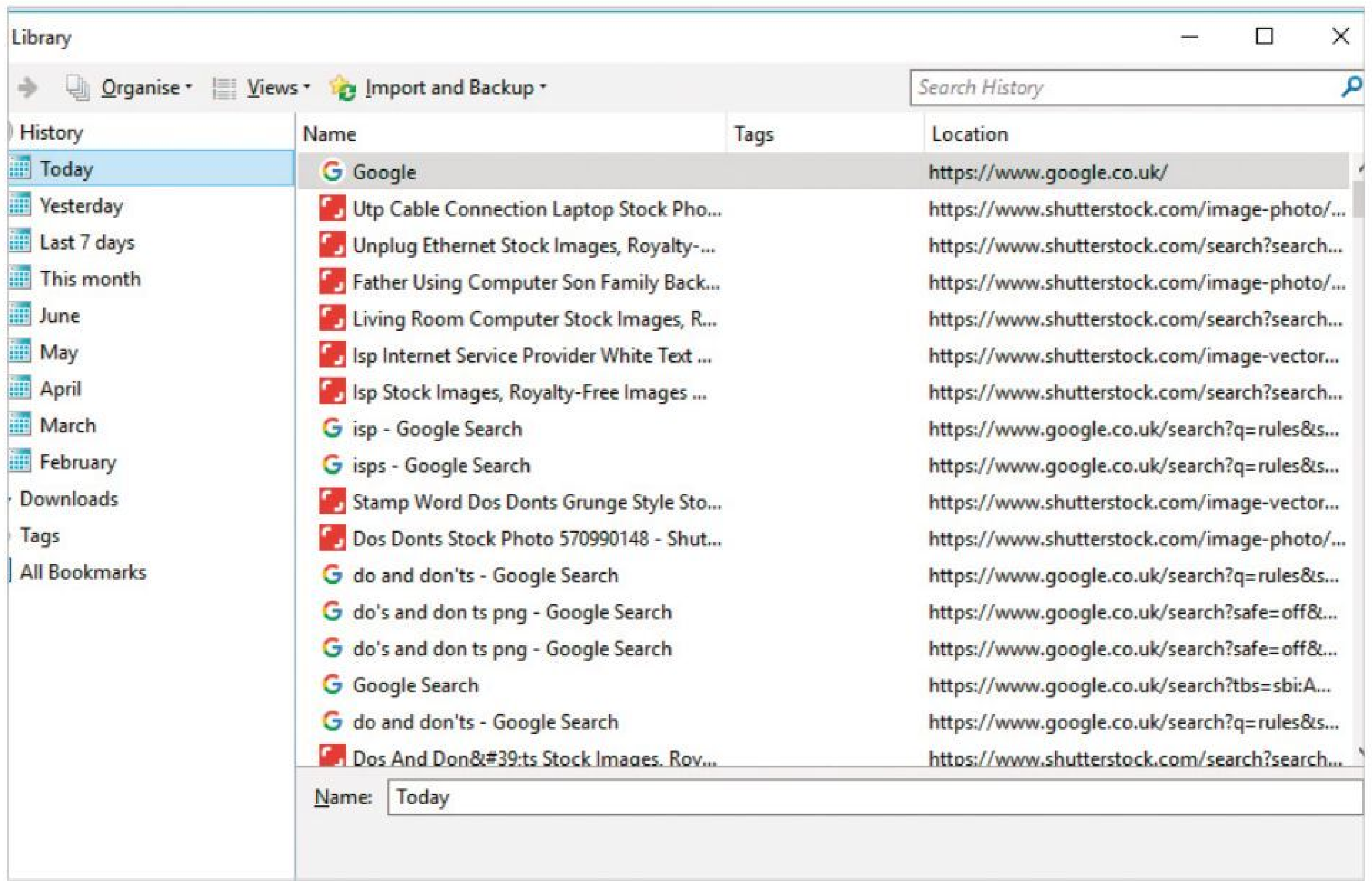
GOING OFFLINE

If your child wants to play a game, one that doesn't involve any online communications, or do some work, consider unplugging the computer or device from the home router. Either pull the cable out of the network port or power down the Wi-Fi. That way they can't get online.



BROWSER HISTORY

After your child has been online, consider taking a look at the browser history. You can find the history among the browser's usual settings, click on the three horizontal bars in the top right of Firefox, for example, followed by History to view the recently visited web pages.

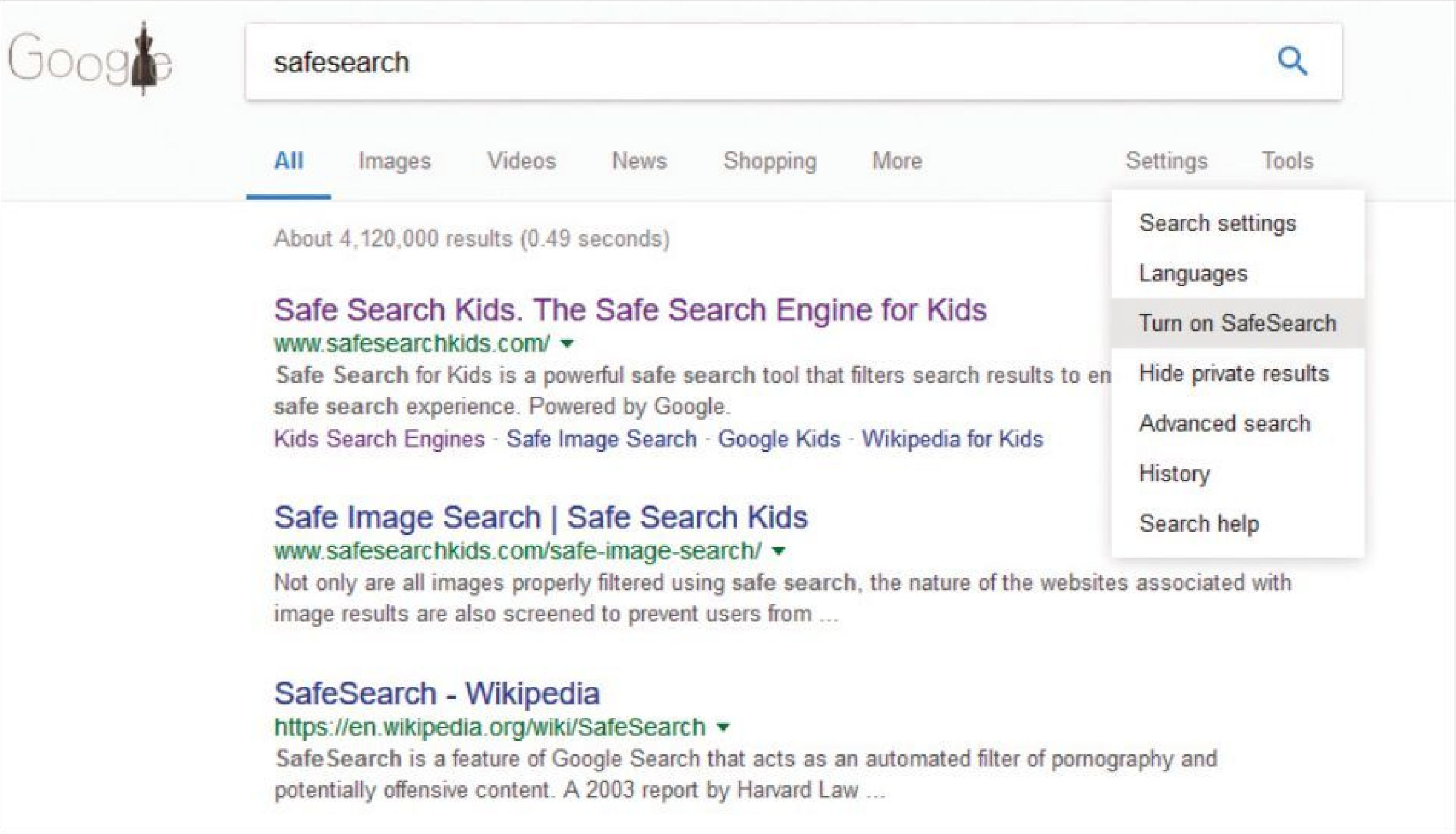


Name	Tags	Location
Google		https://www.google.co.uk/
Utp Cable Connection Laptop Stock Pho...		https://www.shutterstock.com/image-photo/...
Unplug Ethernet Stock Images, Royalty-...		https://www.shutterstock.com/search?search...
Father Using Computer Son Family Back...		https://www.shutterstock.com/image-photo/...
Living Room Computer Stock Images, R...		https://www.shutterstock.com/search?search...
Isp Internet Service Provider White Text ...		https://www.shutterstock.com/image-vector...
Isp Stock Images, Royalty-Free Images ...		https://www.shutterstock.com/search?search...
isp - Google Search		https://www.google.co.uk/search?q=rules&s...
isps - Google Search		https://www.google.co.uk/search?q=rules&s...
Stamp Word Dos Donts Grunge Style Sto...		https://www.shutterstock.com/image-vector...
Dos Donts Stock Photo 570990148 - Shut...		https://www.shutterstock.com/image-photo/...
do and don'ts - Google Search		https://www.google.co.uk/search?q=rules&s...
do's and don ts png - Google Search		https://www.google.co.uk/search?safe=off&...
do's and don ts png - Google Search		https://www.google.co.uk/search?safe=off&...
Google Search		https://www.google.co.uk/search?tbs=sbi:A...
do and don'ts - Google Search		https://www.google.co.uk/search?q=rules&s...
Dos And Don&#39;ts Stock Images, Roy...		https://www.shutterstock.com/search?search...

Name: Today

PARENTAL FILTERS

Make sure that any search engines used, such as Google, have the parental filters set to the maximum or strict levels. In Google, enter something in the search box, then click the Settings link and turn on SafeSearch. Other search engines may differ in appearance but they all have some form of customisable filter rule.



safesearch

About 4,120,000 results (0.49 seconds)

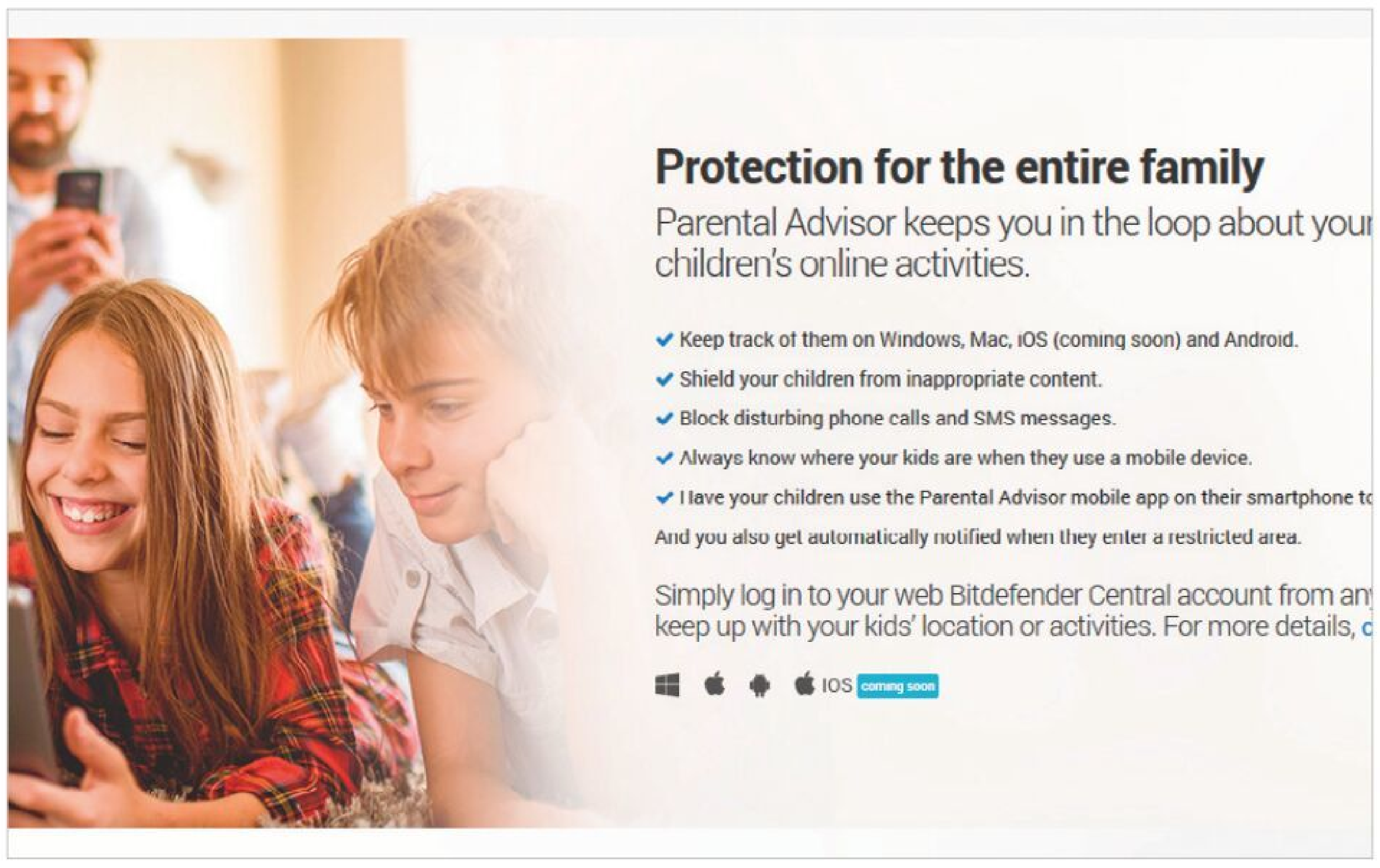
Safe Search Kids. The Safe Search Engine for Kids
www.safesearchkids.com/
Safe Search for Kids is a powerful safe search tool that filters search results to en
safe search experience. Powered by Google.
Kids Search Engines · Safe Image Search · Google Kids · Wikipedia for Kids

Safe Image Search | Safe Search Kids
www.safesearchkids.com/safe-image-search/
Not only are all images properly filtered using safe search, the nature of the websites associated with image results are also screened to prevent users from ...

SafeSearch - Wikipedia
https://en.wikipedia.org/wiki/SafeSearch
SafeSearch is a feature of Google Search that acts as an automated filter of pornography and potentially offensive content. A 2003 report by Harvard Law ...

3RD PARTY SECURITY

It's worth investing in a third-party anti-malware security suite, such as Bitdefender. With Bitdefender, and other security suites, you get some form of family protection allowing you to keep track of Internet use, block unknown communications and even extend the protection to mobile devices.



Protection for the entire family

Parental Advisor keeps you in the loop about your children's online activities.

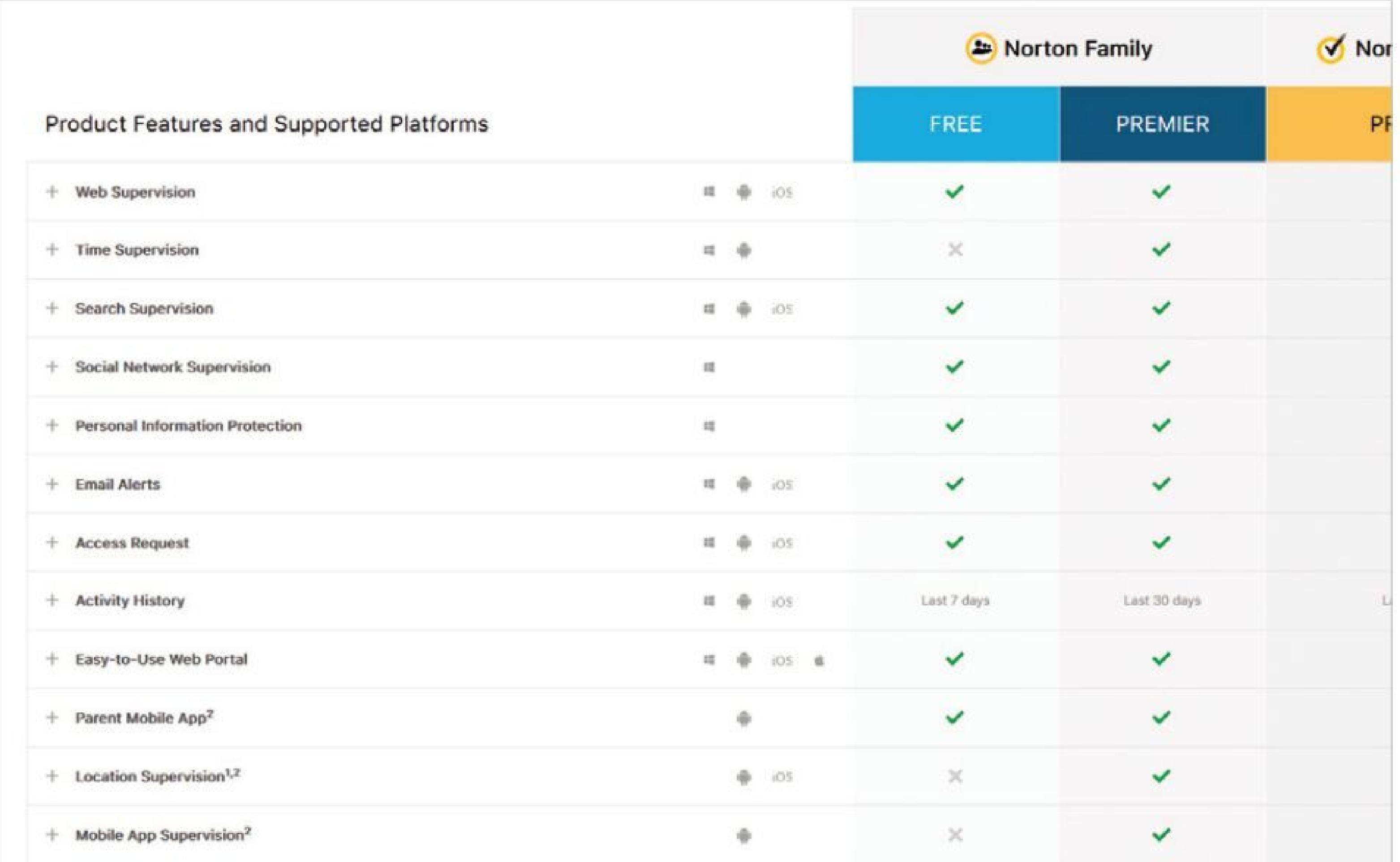
- ✓ Keep track of them on Windows, Mac, iOS (coming soon) and Android.
- ✓ Shield your children from inappropriate content.
- ✓ Block disturbing phone calls and SMS messages.
- ✓ Always know where your kids are when they use a mobile device.
- ✓ Have your children use the Parental Advisor mobile app on their smartphone to

And you also get automatically notified when they enter a restricted area.

Simply log in to your web Bitdefender Central account from an
keep up with your kids' location or activities. For more details,

FREE MONITORING

If you don't want to pay for a full suite, consider using a free monitoring and protection tool such as Norton Family Free Edition. With it you can supervise web access, protect personal information and set up social network supervision.



Product Features and Supported Platforms		Norton Family FREE	Norton Family PREMIER
+ Web Supervision	⊞ ● iOS	✓	✓
+ Time Supervision	⊞ ●	✗	✓
+ Search Supervision	⊞ ● iOS	✓	✓
+ Social Network Supervision	⊞	✓	✓
+ Personal Information Protection	⊞	✓	✓
+ Email Alerts	⊞ ● iOS	✓	✓
+ Access Request	⊞ ● iOS	✓	✓
+ Activity History	⊞ ● iOS	Last 7 days	Last 30 days
+ Easy-to-Use Web Portal	⊞ ● iOS ●	✓	✓
+ Parent Mobile App[2]	●	✓	✓
+ Location Supervision[1,2]	● iOS	✗	✓
+ Mobile App Supervision[2]	●	✗	✓

BECOME FRIENDS

If your child has any social media accounts, make sure to become friends or connected to them. This way you can see what they post, what they like and be ready to help them should something ever get out of hand.

Tips for Technical Guardians to Monitor a Child's Online Activity

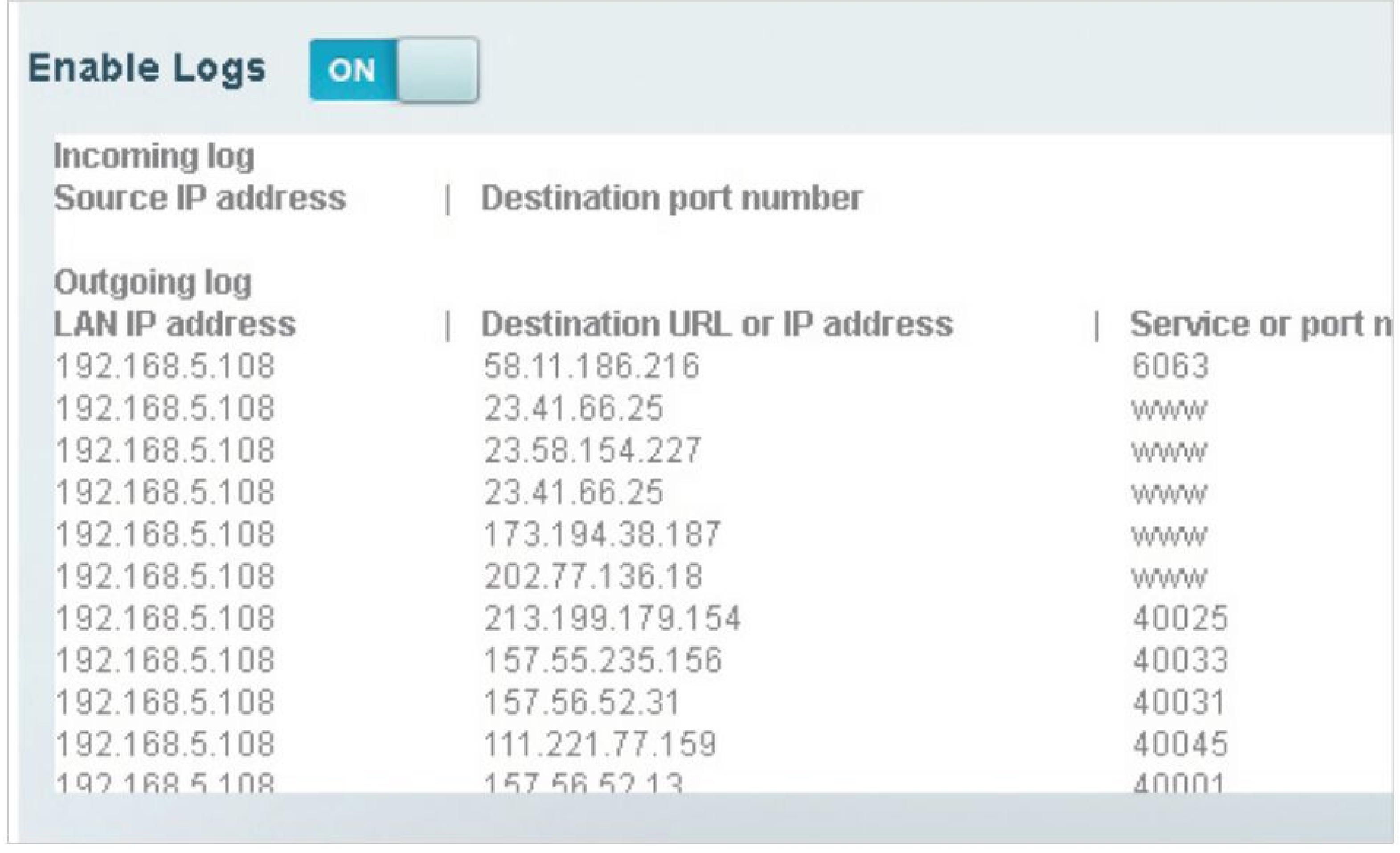
For those parents and guardians who are more technically minded, there's a wealth of software and features available that enable you to monitor your child's Internet activities. Some are simple solutions, others require a little more work, it depends what you're looking for.

Ten Steps for Tech Minded Guardians

As a technically minded parent or guardian, you can monitor traffic, set up batch files to send daily connection reports and fiddle with the inner workings of your router. Here are ten tips to help you out.

ROUTER LOGS

Depending on the router you own, either one you've bought or the ISP-provided one, there's often a way to log web traffic. The logging can sometimes be a single entry detailing the entire house's activity or you can specify individual devices connected to the router. You need to consult your router guide for more information, or contact your ISP.

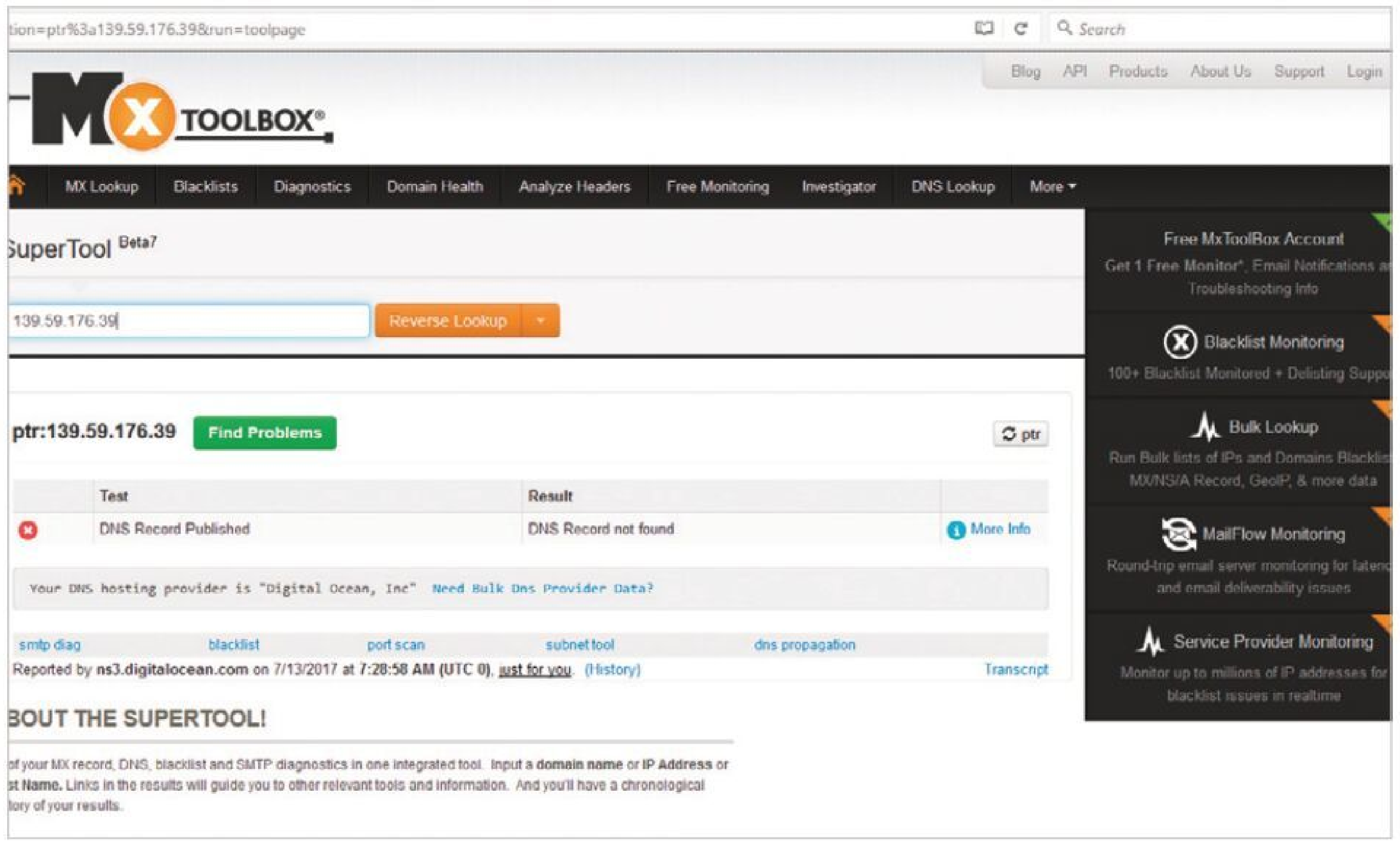


Enable Logs ON

```
Incoming log
Source IP address        | Destination port number

Outgoing log
LAN IP address           | Destination URL or IP address      | Service or port n
192.168.5.108              58.11.186.216                        6063
192.168.5.108              23.41.66.25                          www
192.168.5.108              23.58.154.227                        www
192.168.5.108              23.41.66.25                          www
192.168.5.108              173.194.38.187                       www
192.168.5.108              202.77.136.18                        www
192.168.5.108              213.199.179.154                      40025
192.168.5.108              157.55.235.156                       40033
192.168.5.108              157.56.52.31                         40031
192.168.5.108              111.221.77.159                       40045
192.168.5.108              157.56.52.13                         40001
```

RESOLVE ADDRESSES

If when consulting router logs you have countless IP addresses instead of domain names, you can run the addresses through a reverse IP lookup site. There are dozens available, but MX Toolbox is a good place to start. Enter the IP address and you can see who the hosting company is, and from there ascertain what's being viewed.



MX TOOLBOX
Blog API Products About Us Support Login
MX Lookup Blacklists Diagnostics Domain Health Analyze Headers Free Monitoring Investigator DNS Lookup More
Reverse Lookup
Find Problems
ptr
More Info
Free MxToolBox Account
Blacklist Monitoring
Bulk Lookup
MailFlow Monitoring
Service Provider Monitoring

SuperTool Beta7

139.59.176.39

ptr:139.59.176.39

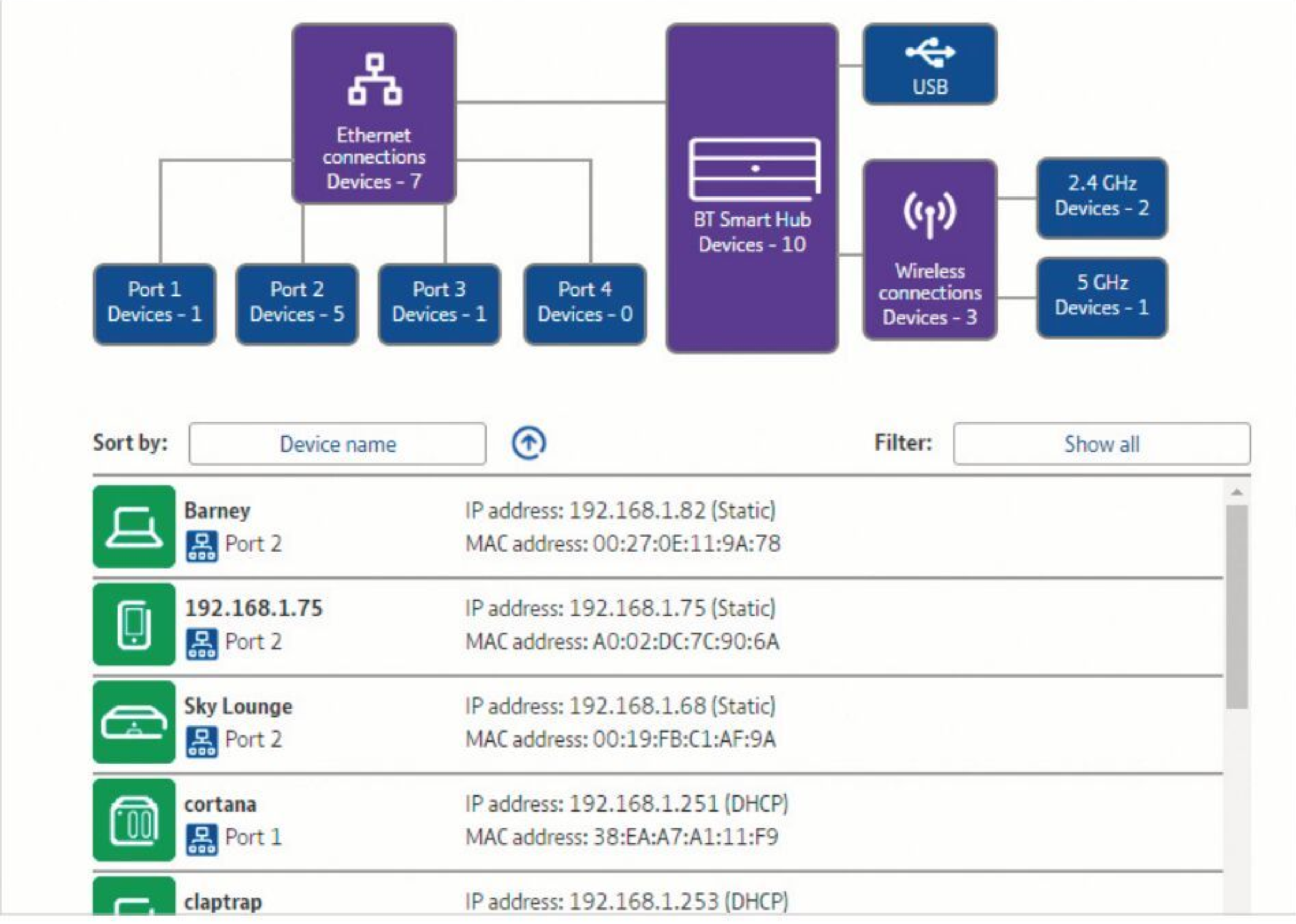
Test	Result
DNS Record Published	DNS Record not found

```
Your DNS hosting provider is "Digital Ocean, Inc"  Need Bulk Dns Provider Data?
```

Reported by ns3.digitalocean.com on 7/13/2017 at 7:28:58 AM (UTC 0), just for you. (History)

FRIENDLY NAMING

This may seem an obvious step but it's one that often overlooked. If you're going to monitor online activity, you need to make sure that the child's devices are correctly labelled in the router setup. Instead of them being just a string of numbers, take the time to ensure they're labelled as 'Bobby's iPad' and so on.



Ethernet connections Devices - 7
BT Smart Hub Devices - 10
USB
Wireless connections Devices - 3
2.4 GHz Devices - 2
5 GHz Devices - 1
Port 1 Devices - 1
Port 2 Devices - 5
Port 3 Devices - 1
Port 4 Devices - 0

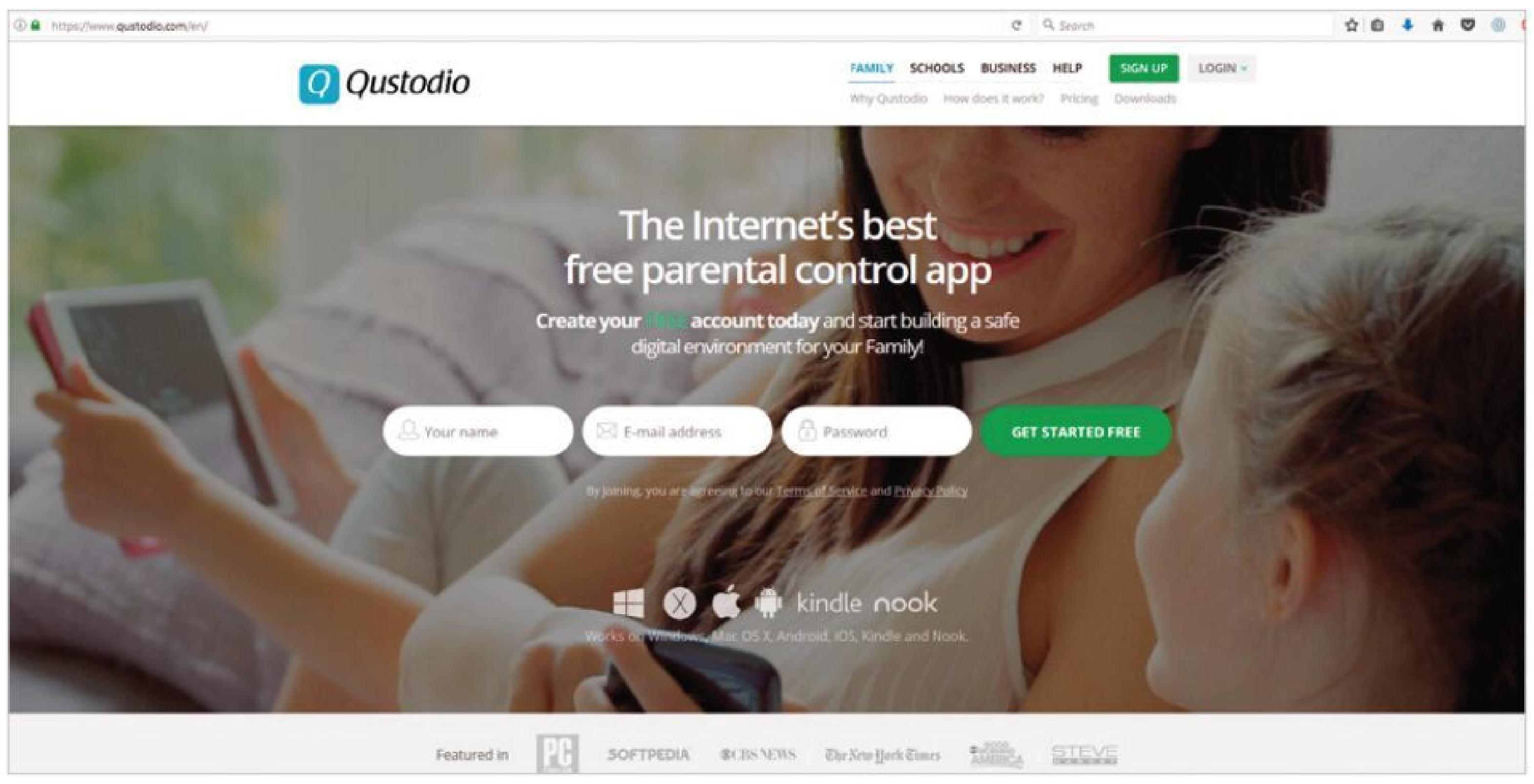
Sort by: Device name

Filter: Show all

Barney Port 2	IP address: 192.168.1.82 (Static) MAC address: 00:27:0E:11:9A:78
192.168.1.75 Port 2	IP address: 192.168.1.75 (Static) MAC address: A0:02:DC:7C:90:6A
Sky Lounge Port 2	IP address: 192.168.1.68 (Static) MAC address: 00:19:FB:C1:AF:9A
cortana Port 1	IP address: 192.168.1.251 (DHCP) MAC address: 38:EA:A7:A1:11:F9
claptrap	IP address: 192.168.1.253 (DHCP)

PARENTAL MONITORING

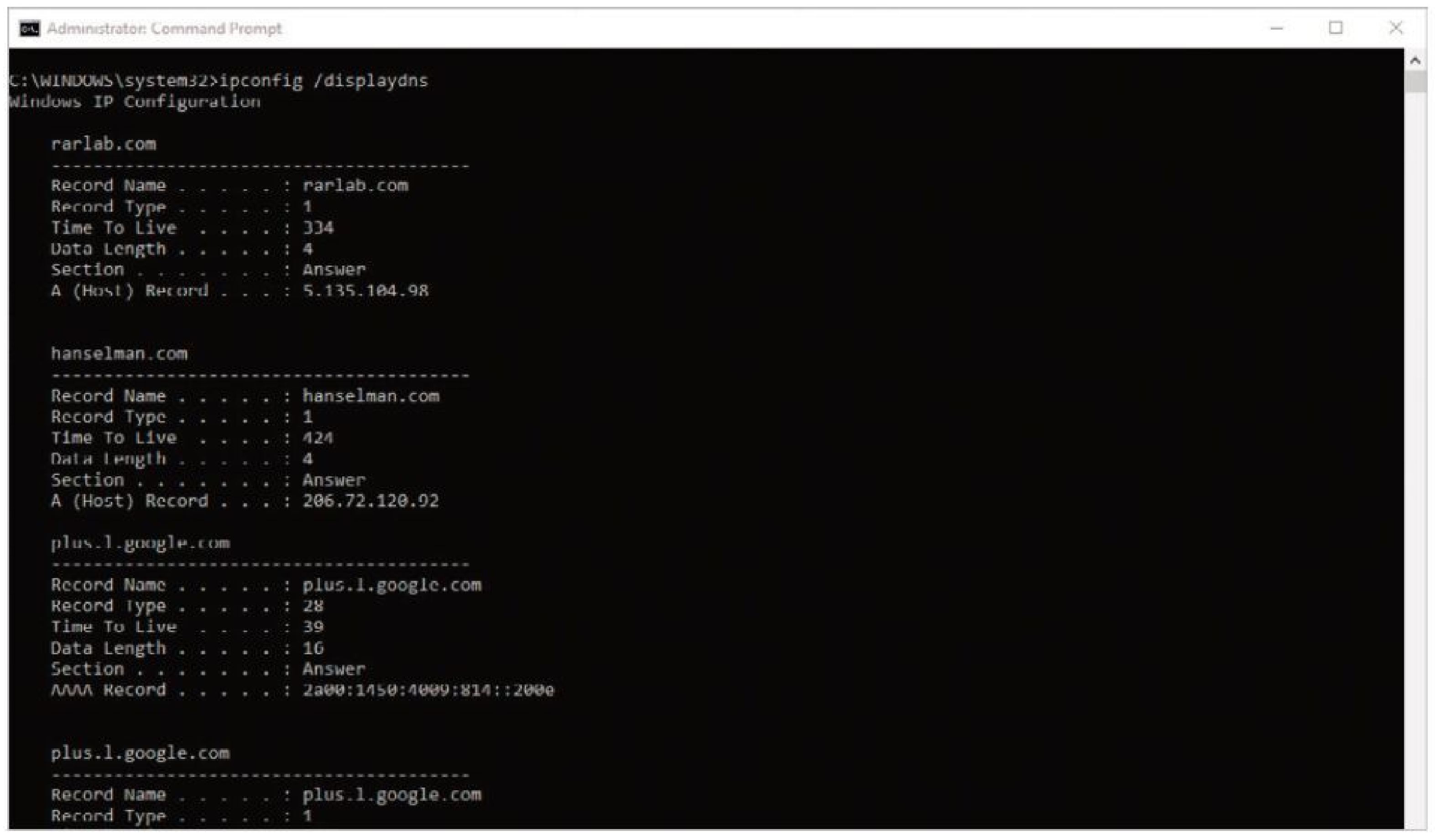
Monitoring software is a must have for parents or guardians who want to limit and control what their children do online. We'll look at some examples over the page but to begin with take a look at Qustodio Parental Control: **https://.qustodio.com/en/**. It's a cross-platform tool for better monitoring of online activity, and it's reasonably well priced.



Qustodio
FAMILY SCHOOLS BUSINESS HELP SIGN UP LOGIN
Why Qustodio How does it work? Pricing Downloads
The Internet's best
free parental control app
Create your FREE account today and start building a safe digital environment for your Family!
Your name
E-mail address
Password
GET STARTED FREE
kindle nook
Featured in
SOFTPEDIA

DISPLAY DNS

For those who like to get their hands dirty in the command line, open up CMD from the Windows Start button and enter the command: **ipconfig /displaydns**. This will list the sites visited by the user during their session. If you want, record the sites to a text file for viewing later with, for example: **ipconfig /displaydns > c:\monitoring\sites.txt**.

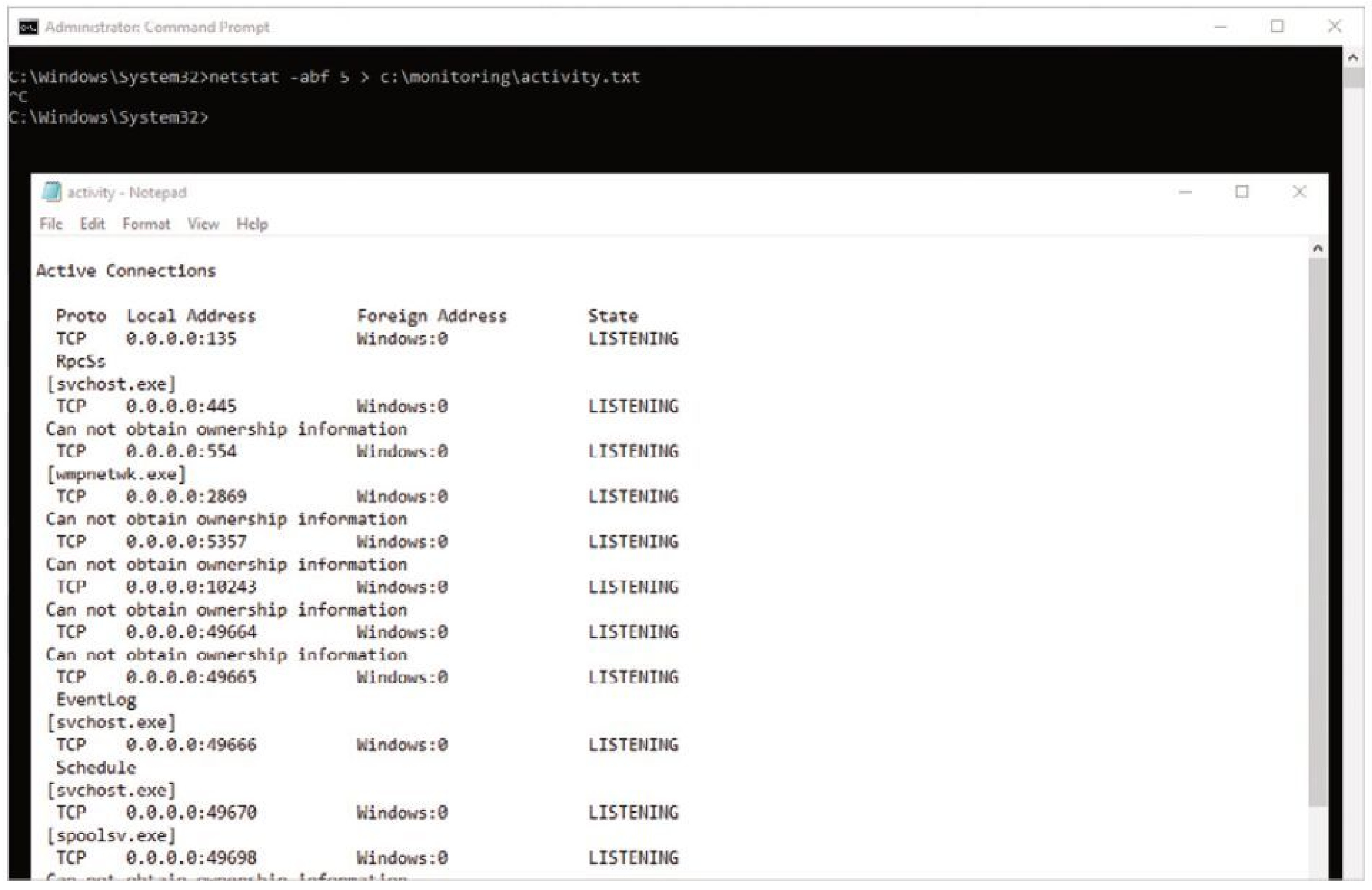


Administrator: Command Prompt

```
C:\WINDOWS\system32>ipconfig /displaydns
Windows IP Configuration

    rarlab.com
    ----------------------------------------
    Record Name . . . . . : rarlab.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 334
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 5.135.104.98


    hanselman.com
    ----------------------------------------
    Record Name . . . . . : hanselman.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 424
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 206.72.120.92

    plus.l.google.com
    ----------------------------------------
    Record Name . . . . . : plus.l.google.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 39
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2a00:1450:4009:814::200e


    plus.l.google.com
    ----------------------------------------
    Record Name . . . . . : plus.l.google.com
    Record Type . . . . . : 1
```

NETSTAT COMMAND

Using the Netstat command that we looked at on page 98, you can enter into a command prompt: **netstat -abf 5 > c:\monitoring\activity.txt**. This will record the entire activity of a session to a file, which you can then browse. The recording will stop once the child has logged out of their Windows account.



Administrator: Command Prompt

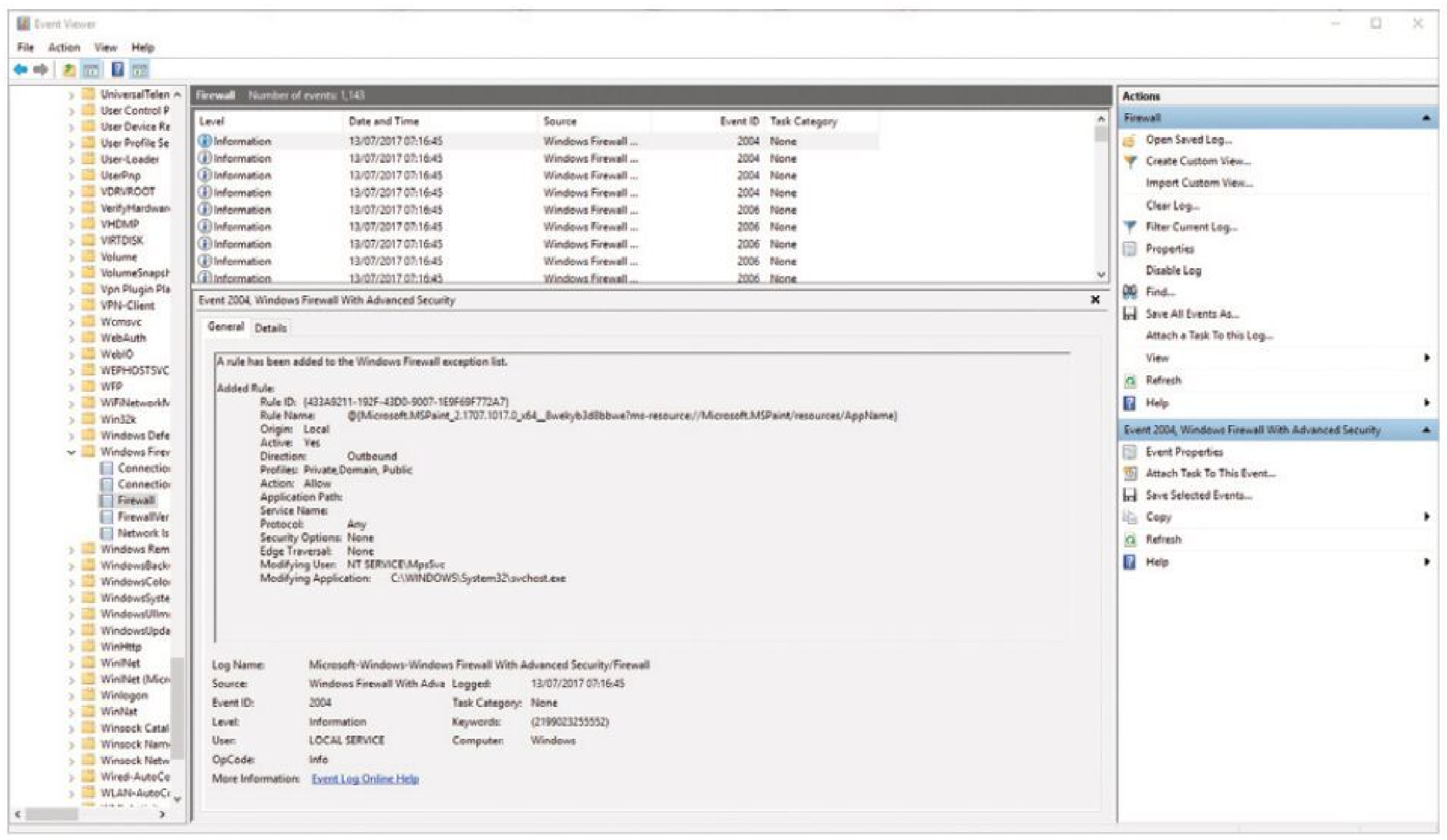
```
C:\Windows\System32>netstat -abf 5 > c:\monitoring\activity.txt
^C
C:\Windows\System32>
```

activity - Notepad

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Windows:0              LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:554            Windows:0              LISTENING
 [wmpnetwk.exe]
  TCP    0.0.0.0:2869           Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:5357           Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:10243          Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49664          Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49665          Windows:0              LISTENING
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49666          Windows:0              LISTENING
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49670          Windows:0              LISTENING
 [spoolsv.exe]
  TCP    0.0.0.0:49698          Windows:0              LISTENING
```

WINDOWS LOGS

Don't forget to check your Windows Event Logs, especially the Windows Firewall Event Log for any activity that may have triggered the Firewall. You can then build up a picture of where the child is visiting that's causing the Firewall to react and educate them in the dangers of malware and such.



Event Viewer

Firewall Number of events: 1,143

Level	Date and Time	Source	Event ID	Task Category
Information	13/07/2017 07:16:45	Windows Firewall ...	2004	None
Information	13/07/2017 07:16:45	Windows Firewall ...	2004	None
Information	13/07/2017 07:16:45	Windows Firewall ...	2004	None
Information	13/07/2017 07:16:45	Windows Firewall ...	2004	None
Information	13/07/2017 07:16:45	Windows Firewall ...	2006	None
Information	13/07/2017 07:16:45	Windows Firewall ...	2006	None
Information	13/07/2017 07:16:45	Windows Firewall ...	2006	None
Information	13/07/2017 07:16:45	Windows Firewall ...	2006	None
Information	13/07/2017 07:16:45	Windows Firewall ...	2006	None

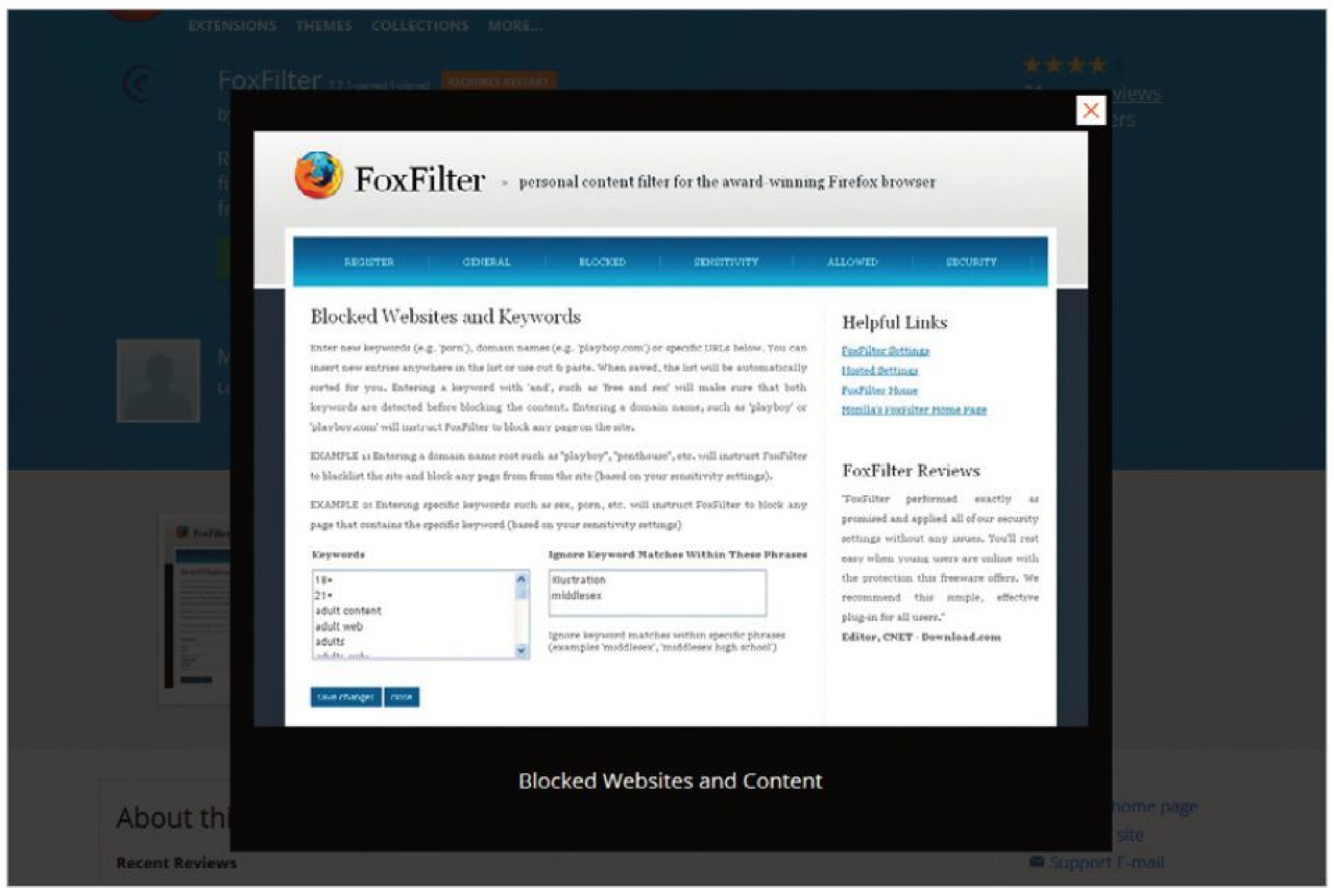
Event 2004, Windows Firewall With Advanced Security

```
A rule has been added to the Windows Firewall exception list.

Added Rule:
        Rule ID:    {433A9211-192F-43D0-9007-1E9F69F772A7}
        Rule Name:      @{Microsoft.MSPaint_2.1707.1017.0_x64__8wekyb3d8bbwe?ms-resource://Microsoft.MSPaint/resources/AppName}
        Origin:   Local
        Active:   Yes
        Direction:      Outbound
        Profiles:  Private,Domain, Public
        Action:   Allow
        Application Path:
        Service Name:
        Protocol:       Any
        Security Options: None
        Edge Traversal:   None
        Modifying User:   NT SERVICE\MpsSvc
        Modifying Application:     C:\WINDOWS\System32\svchost.exe
```

Log Name: Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
Source: Windows Firewall With Adva
Logged: 13/07/2017 07:16:45
Event ID: 2004
Task Category: None
Level: Information
Keywords: (2199023255552)
User: LOCAL SERVICE
Computer: Windows
OpCode: Info
More Information: Event Log Online Help

BROWSER CONTROL

If you need a specific monitoring and parental control tool, then consider using FoxFilter for Firefox. This is an add-on that can block customised websites, such as anything containing inappropriate content and report its use in a handy web interface.



FoxFilter » personal content filter for the award-winning Firefox browser

Blocked Websites and Keywords

Enter new keywords (e.g. 'porn'), domain names (e.g. 'playboy.com') or specific URLs below. You can insert new entries anywhere in the list or use cut & paste. When saved, the list will be automatically sorted for you. Entering a keyword with 'and', such as 'free and sex' will make sure that both keywords are detected before blocking the content. Entering a domain name, such as 'playboy' or 'playboy.com' will instruct FoxFilter to block any page on the site.

EXAMPLE 1: Entering a domain name root such as "playboy", "penthouse", etc. will instruct FoxFilter to blacklist the site and block any page from from the site (based on your sensitivity settings).

EXAMPLE 2: Entering specific keywords such as sex, porn, etc. will instruct FoxFilter to block any page that contains the specific keyword (based on your sensitivity settings)

Keywords: 18+, 21+, adult content, adult web, adults

Ignore Keyword Matches Within These Phrases: illustration, middlesex

Ignore keyword matches within specific phrases (examples 'middlesex', 'middlesex high school')

Helpful Links

FoxFilter Settings
Hosted Settings
FoxFilter Home
Mozilla's FoxFilter Home Page

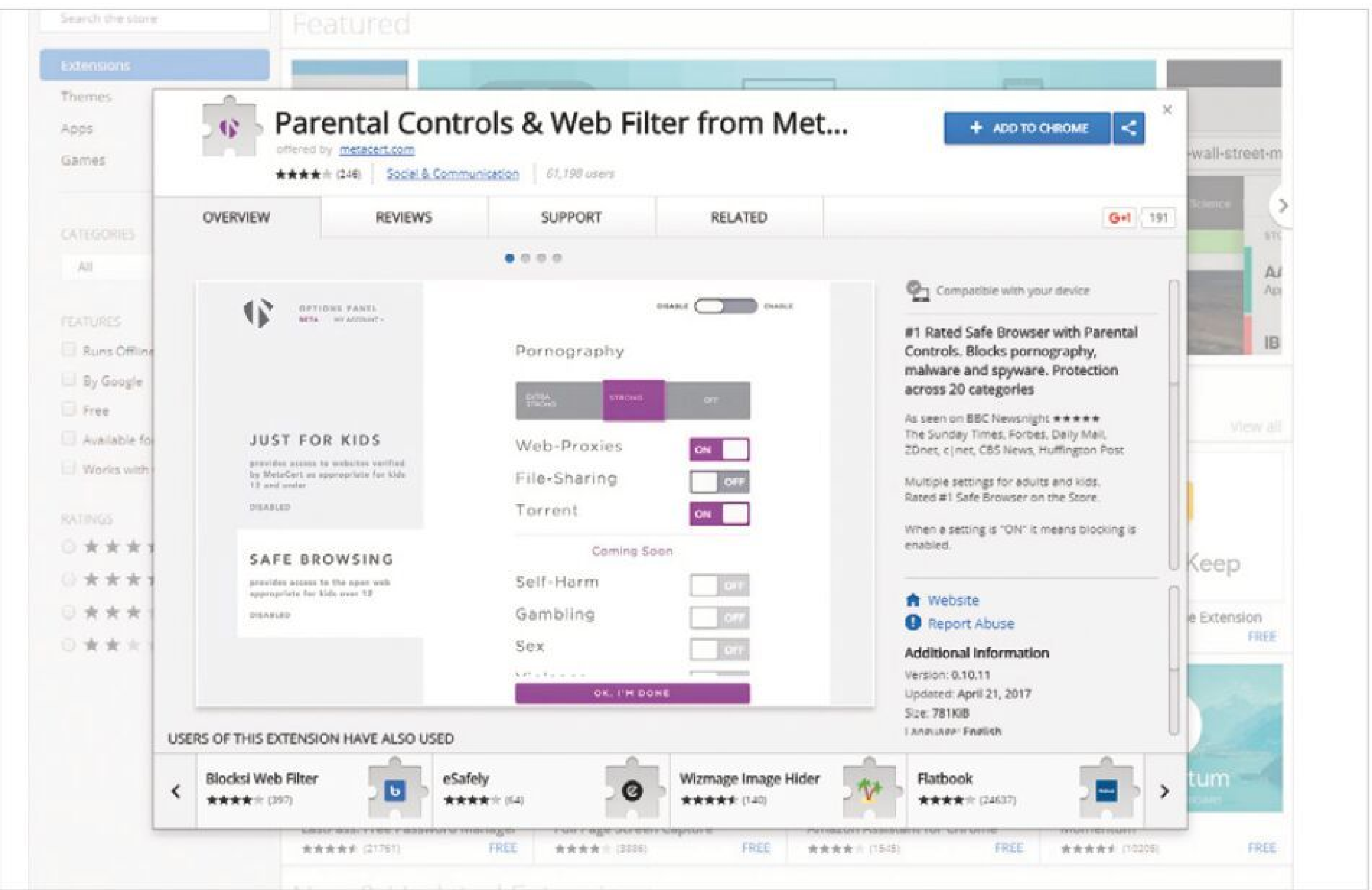
FoxFilter Reviews

"FoxFilter performed exactly as promised and applied all of our security settings without any issues. You'll rest easy when young users are online with the protection this freeware offers. We recommend this simple, effective plug-in for all users."
Editor, CNET - Download.com

Blocked Websites and Content

CHROME CONTROL

Users of Chrome can try MetaCert's Parental Controls & Web Filtering add-on. With it you can block certain sites, set profiles and monitor the web activity of your child as they use the browser. There are plenty of features, so it's worth looking over if you regularly use Chrome.



Parental Controls & Web Filter from Met...
offered by metacert.com
★★★★ (246) | Social & Communication | 61,198 users

Compatible with your device

#1 Rated Safe Browser with Parental Controls. Blocks pornography, malware and spyware. Protection across 20 categories

As seen on BBC Newsnight ★★★★★ The Sunday Times, Forbes, Daily Mail, ZDnet, c|net, CBS News, Huffington Post

Multiple settings for adults and kids. Rated #1 Safe Browser on the Store.

When a setting is "ON" it means blocking is enabled.

Website
Report Abuse

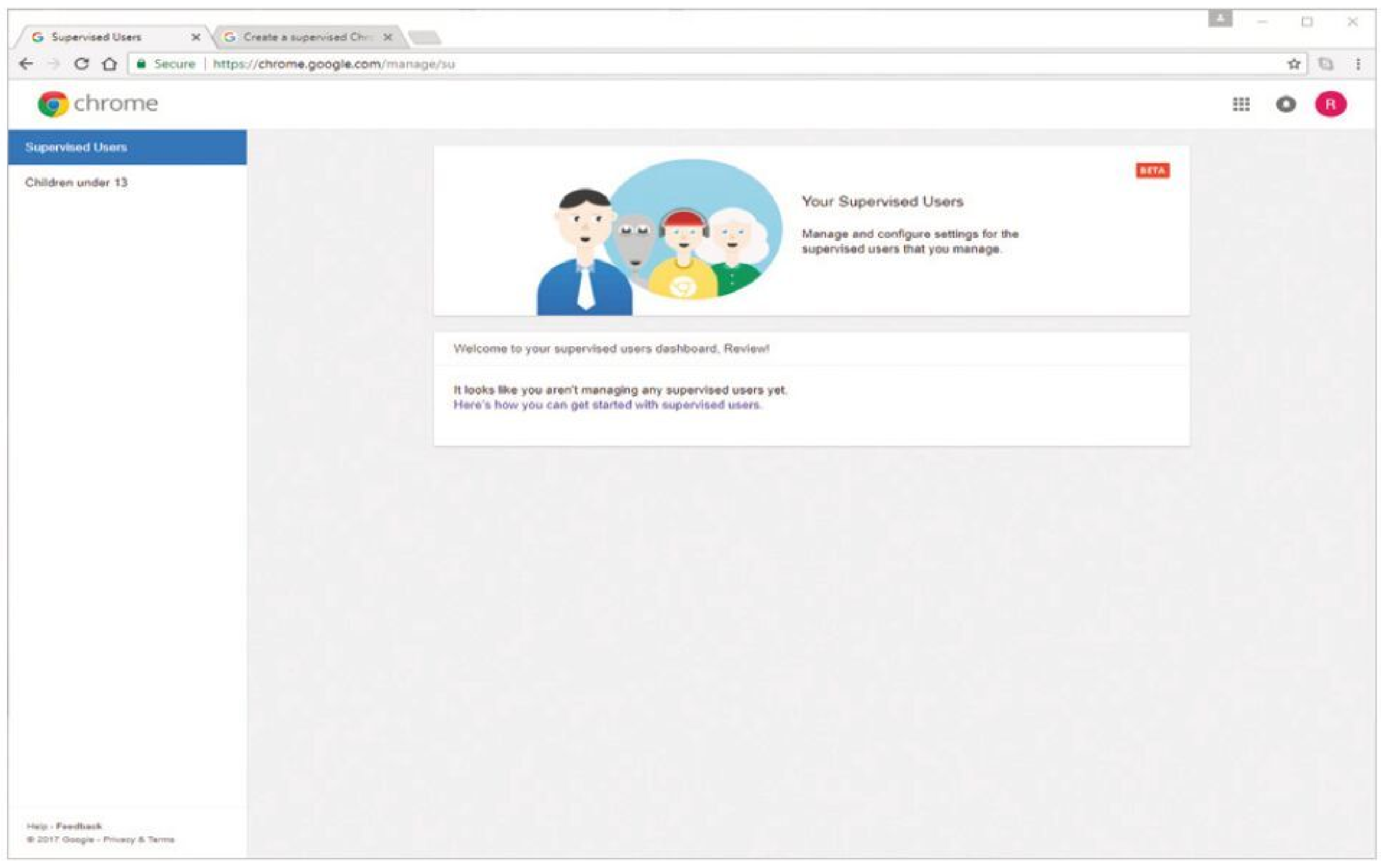
Additional Information
Version: 0.10.11
Updated: April 21, 2017
Size: 781KiB
Language: English

USERS OF THIS EXTENSION HAVE ALSO USED

Blocksi Web Filter ★★★★ (397)
eSafely ★★★★ (64)
Wizmage Image Hider ★★★★★ (140)
Flatbook ★★★★ (24637)

SUPERVISED USER

While still on Chrome users, if you visit **http://chrome.com/manage**, you're able to set up a supervised user for the other Chrome accounts. This way you can set restrictions and monitor the sites that a user has visited during their Chrome use.



https://chrome.google.com/manage/su

Your Supervised Users

Manage and configure settings for the supervised users that you manage.

Welcome to your supervised users dashboard, Review!

It looks like you aren't managing any supervised users yet.
Here's how you can get started with supervised users.

Ten Monitoring Tools to Install and Use

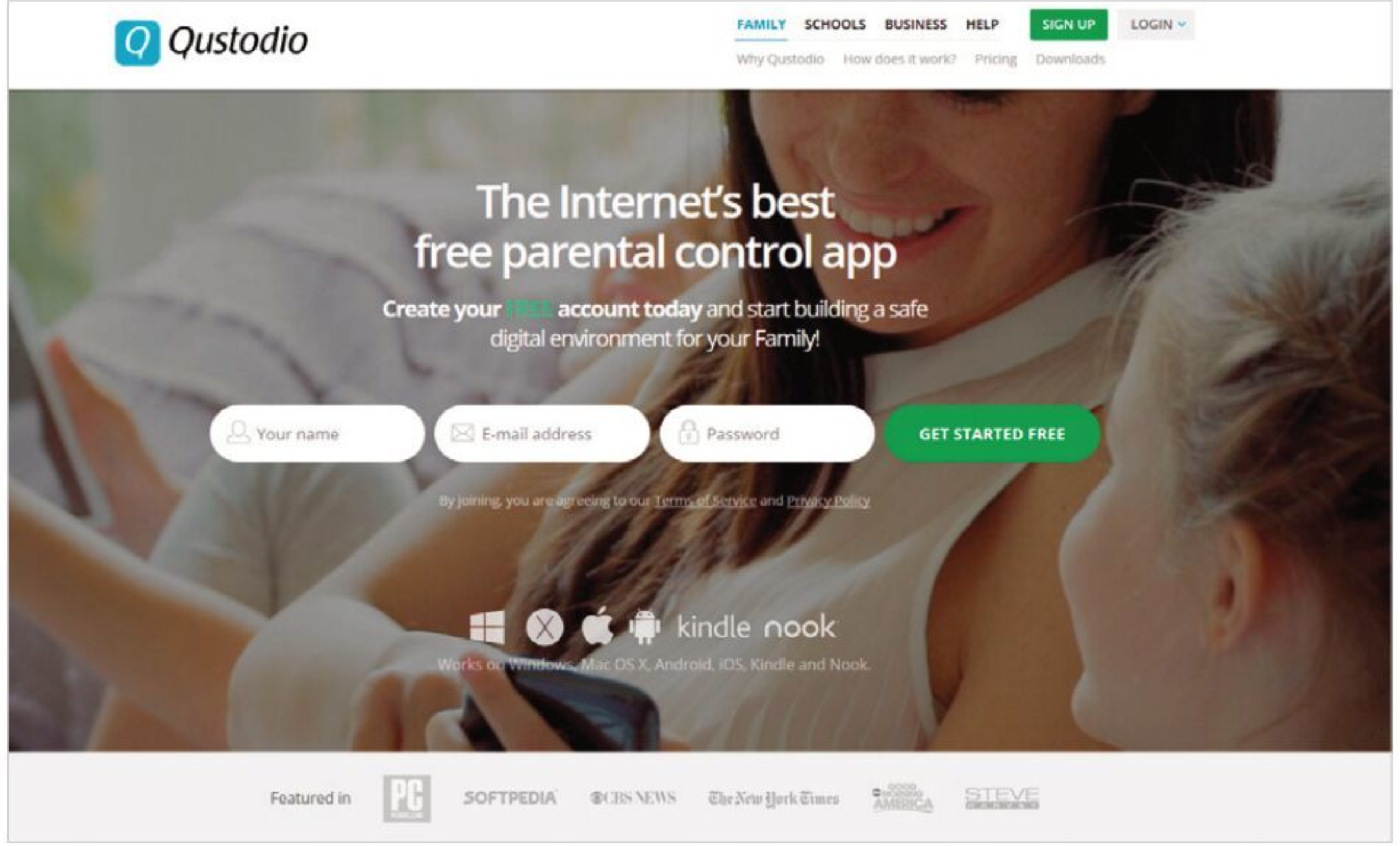
Monitoring tools usually come within a complete Parental Control package. These tools can be dedicated programs, or come as a part of a security suite. Either way, they're excellent ways to help keep children and young people safe on the Internet.

Parental Controls

We've collated ten of the better parental control and monitoring tools and software, in no particular order. Some offer their software for free, others you need to pay for.

QUSTODIO

We've mentioned Qustodio in the previous page, so it's a good example to kick of this top ten tools section with. Qustodio is a complete package that monitors, blocks, filters and controls times, games and apps across many different platforms. Pricing for up to five devices starts at £32.95 per year.


Qustodio
FAMILY
SCHOOLS
BUSINESS
HELP
SIGN UP
LOGIN
Why Qustodio
How does it work?
Pricing
Downloads
Your name
E-mail address
Password
GET STARTED FREE
kindle
nook
Featured in
SOFTPEDIA
CBS NEWS
The New York Times

The Internet's best free parental control app

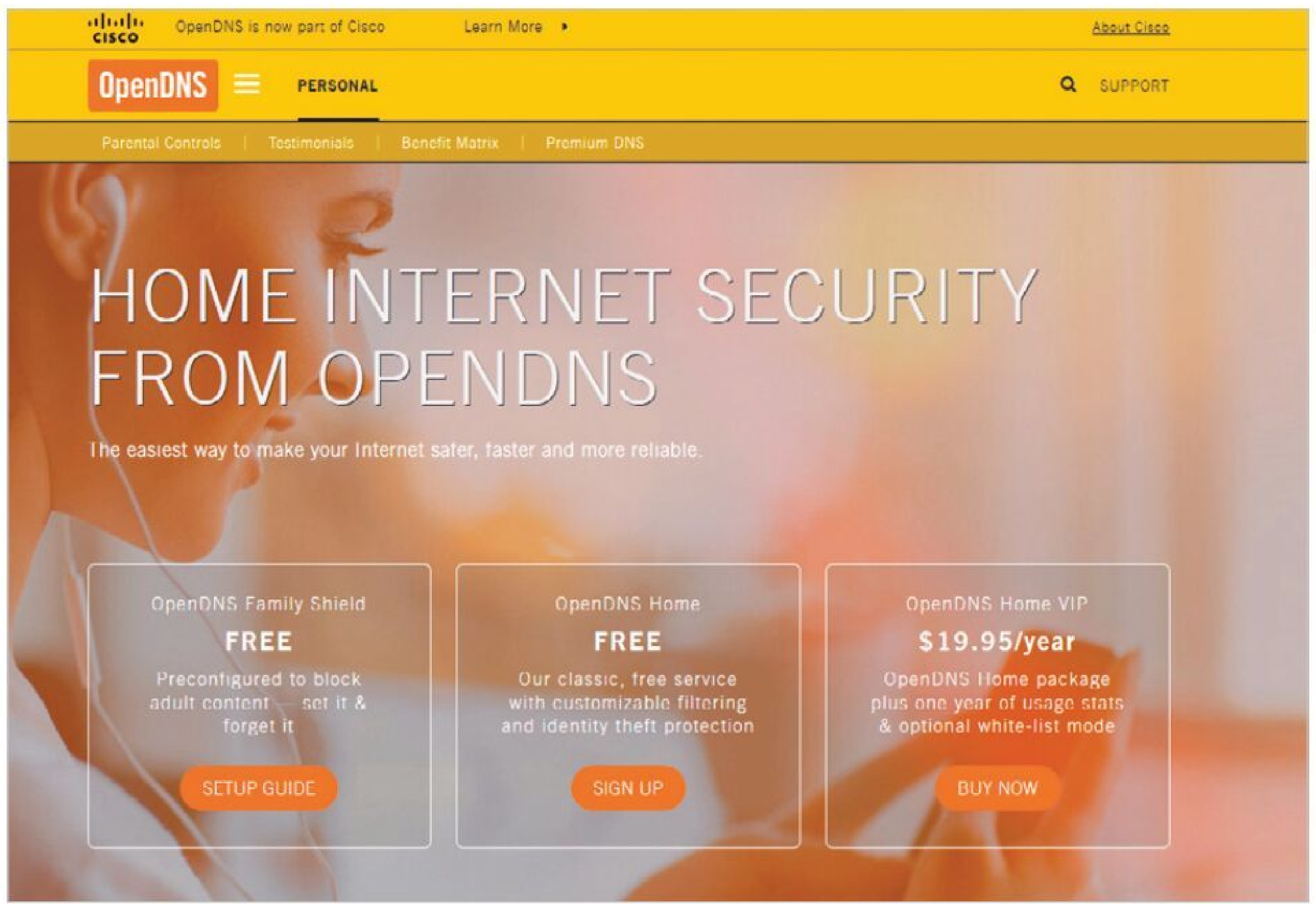
Create your FREE account today and start building a safe digital environment for your Family!

By joining, you are agreeing to our Terms of Service and Privacy Policy

Works on Windows, Mac OS X, Android, iOS, Kindle and Nook.

OPENDNS

OpenDNS from Cisco offers both free and paid-for services to help block inappropriate content across virtually any Internet connected device. You need to set up DNS entries in your router to take advantage of it but full instructions are given via a helpful setup guide.


CISCO
OpenDNS is now part of Cisco
Learn More
About Cisco
OpenDNS
PERSONAL
SUPPORT
Parental Controls
Testimonials
Benefit Matrix
Premium DNS
SETUP GUIDE
SIGN UP
BUY NOW

HOME INTERNET SECURITY FROM OPENDNS

The easiest way to make your Internet safer, faster and more reliable.

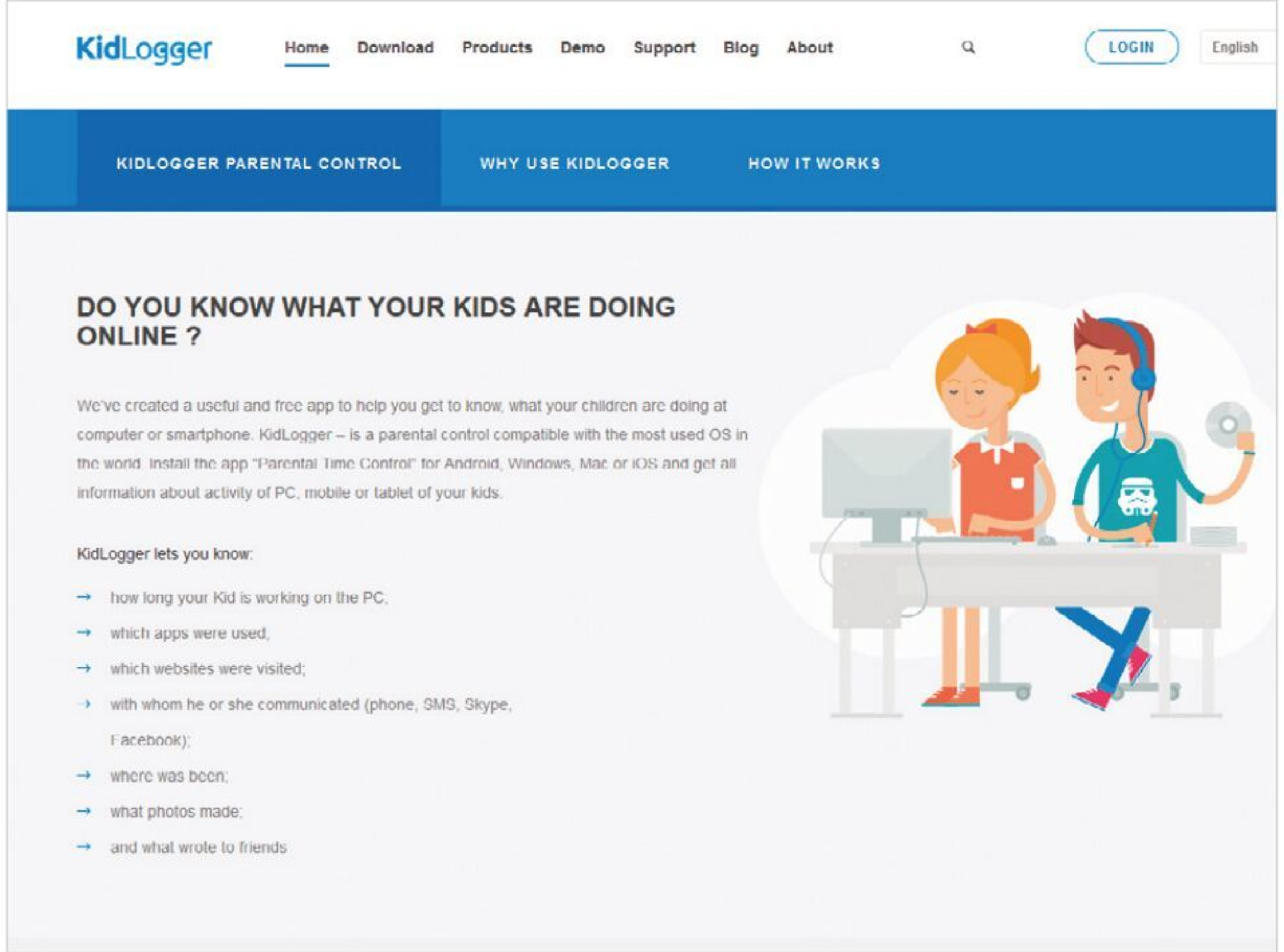
OpenDNS Family Shield
FREE
Preconfigured to block adult content — set it & forget it

OpenDNS Home
FREE
Our classic, free service with customizable filtering and identity theft protection

OpenDNS Home VIP
$19.95/year
OpenDNS Home package plus one year of usage stats & optional white-list mode

KIDLOGGER

KidLogger is an interesting product that offers a basic, single device with nine days of history for free, moving up to five devices, then ten devices for increasing costs. You can monitor browser activities across Windows, Mac and Android; block apps, take screenshots and limit time, amongst other features.


KidLogger
Home
Download
Products
Demo
Support
Blog
About
LOGIN
English
KIDLOGGER PARENTAL CONTROL
WHY USE KIDLOGGER
HOW IT WORKS

DO YOU KNOW WHAT YOUR KIDS ARE DOING ONLINE ?

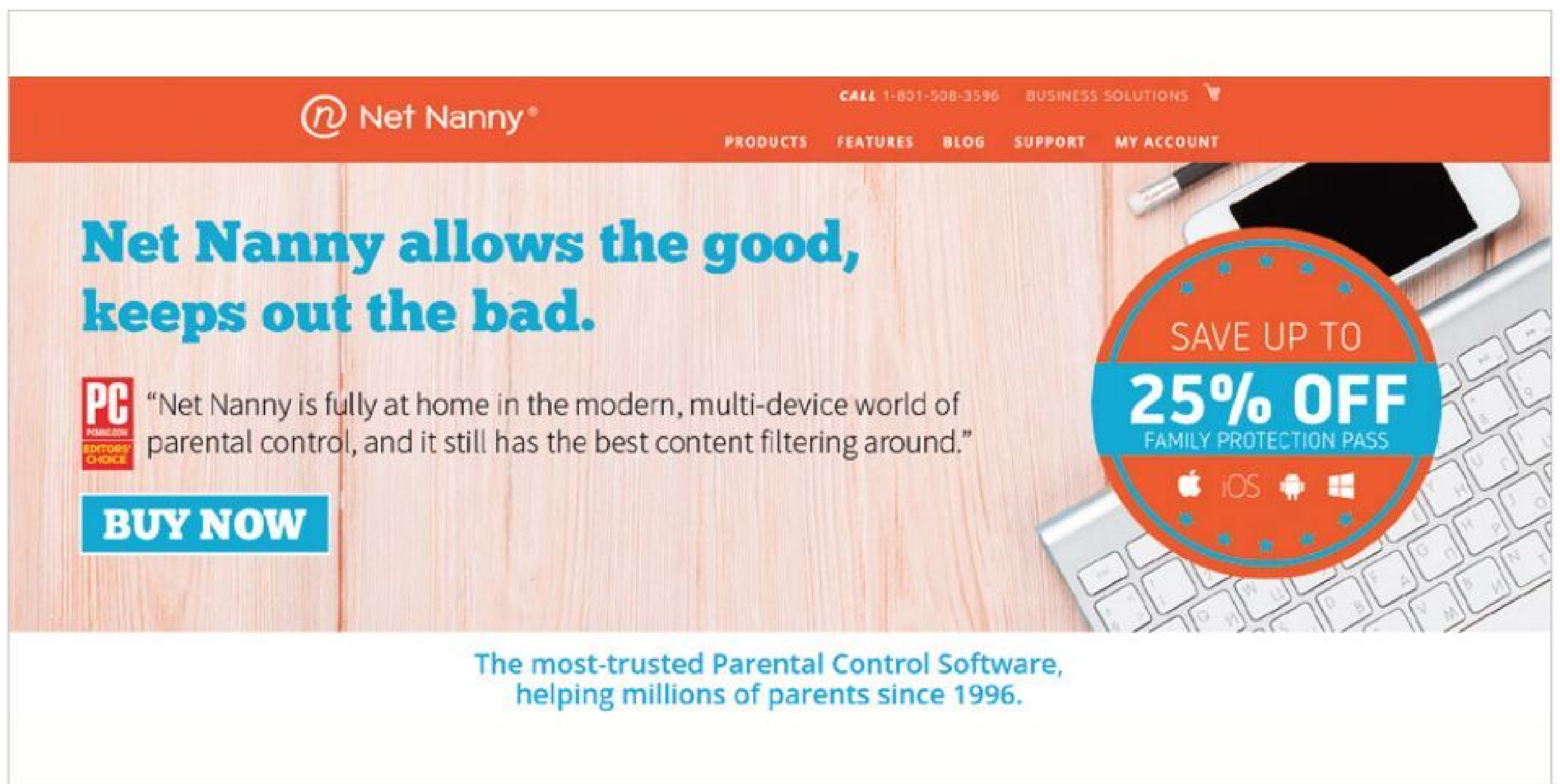
We've created a useful and free app to help you get to know, what your children are doing at computer or smartphone. KidLogger – is a parental control compatible with the most used OS in the world. Install the app "Parental Time Control" for Android, Windows, Mac or iOS and get all information about activity of PC, mobile or tablet of your kids.

KidLogger lets you know:

→ how long your Kid is working on the PC,
→ which apps were used,
→ which websites were visited;
→ with whom he or she communicated (phone, SMS, Skype, Facebook);
→ where was been;
→ what photos made;
→ and what wrote to friends

NET NANNY

Without a doubt, one of the most respected parental control solutions available is Net Nanny. It's been around since 1996 and offers unparalleled levels of filtering, protection, monitoring and parental controls. It's cross-platform and prices vary depending on what you want, so it's best to check out the latest offers available.

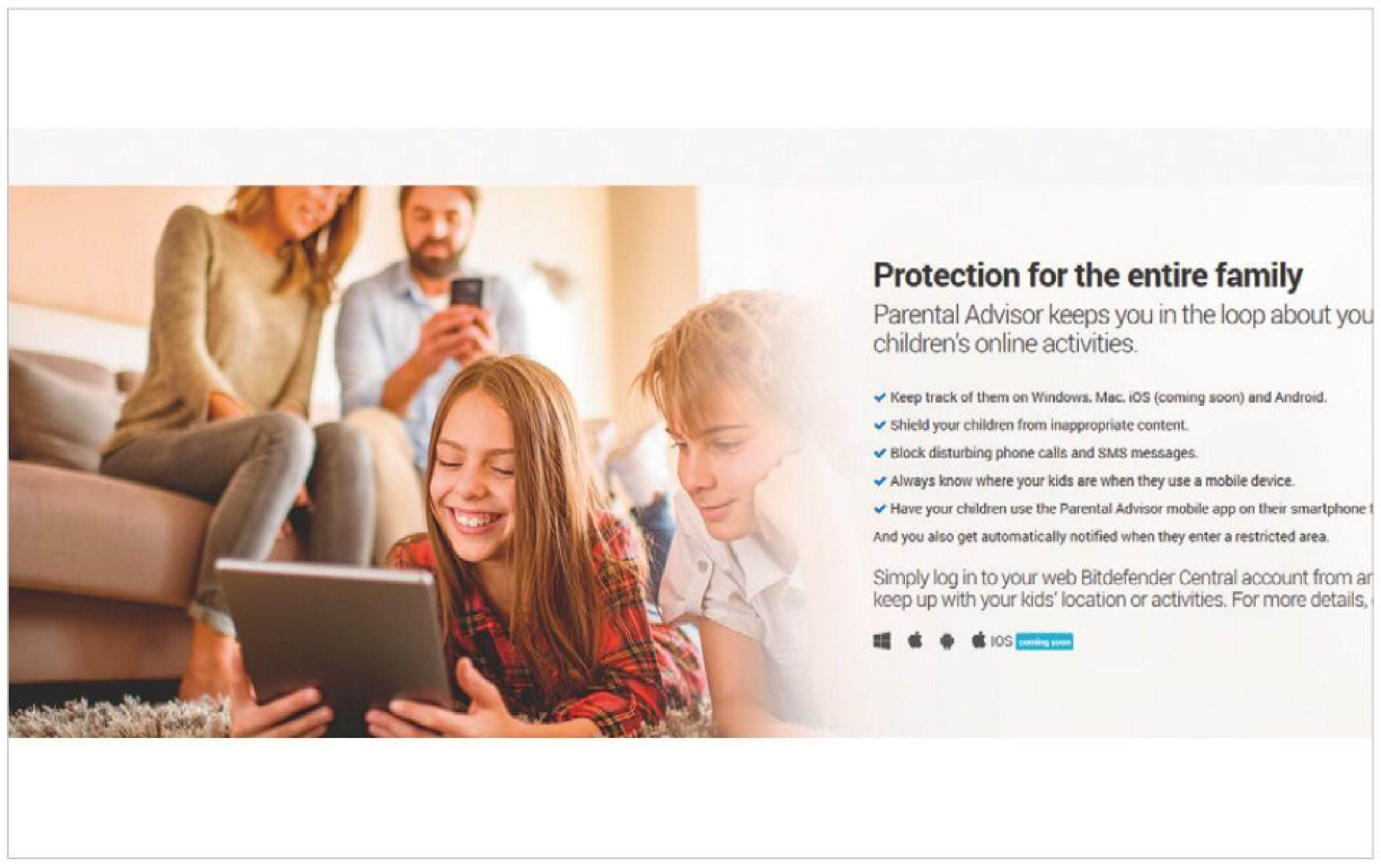

Net Nanny®
CALL 1-801-508-3596
BUSINESS SOLUTIONS
PRODUCTS
FEATURES
BLOG
SUPPORT
MY ACCOUNT
Net Nanny allows the good, keeps out the bad.
PC EDITORS' CHOICE
BUY NOW
SAVE UP TO
25% OFF
FAMILY PROTECTION PASS
iOS

"Net Nanny is fully at home in the modern, multi-device world of parental control, and it still has the best content filtering around."

The most-trusted Parental Control Software, helping millions of parents since 1996.

BITDEFENDER

Bitdefender's Total Security suite offers an excellent parental control and monitoring tool within it's already impressive list of features. It's cross-platform, can shield children and young people from inappropriate content and extends its use to mobile devices too. Pricing starts at just £34.99.



Protection for the entire family

Parental Advisor keeps you in the loop about you children's online activities.

- Keep track of them on Windows, Mac, iOS (coming soon) and Android.
- Shield your children from inappropriate content.
- Block disturbing phone calls and SMS messages.
- Always know where your kids are when they use a mobile device.
- Have your children use the Parental Advisor mobile app on their smartphone

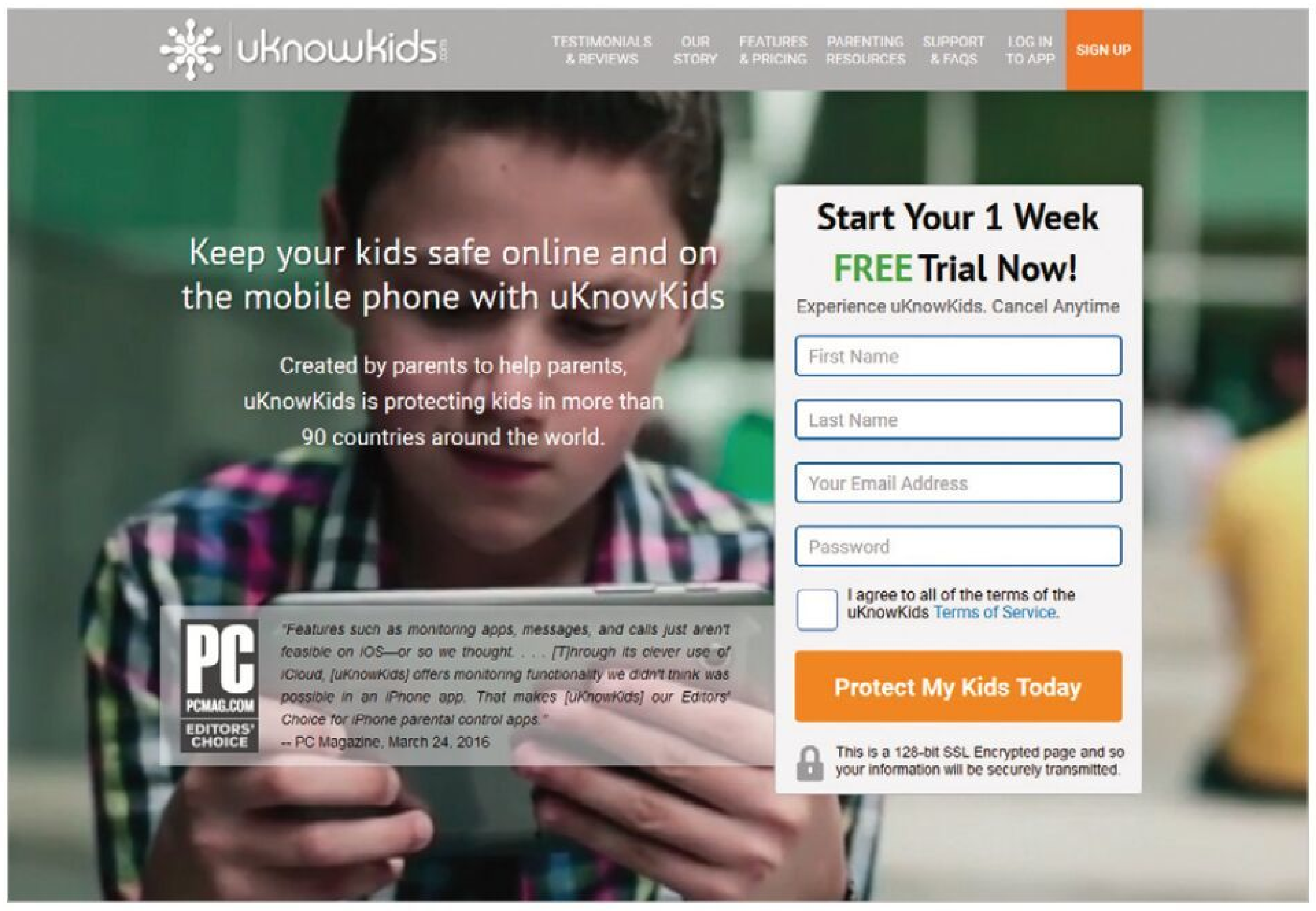
And you also get automatically notified when they enter a restricted area.

Simply log in to your web Bitdefender Central account from ar keep up with your kids' location or activities. For more details,

iOS
coming soon

UKNOWKIDS

uKnowKids provides a wealth of features for parents, including call logging on devices (with Facetime call logs), image reviews that children post, social media monitoring and web browsing history access and controls to block inappropriate content. Pricing varies, so it's best to visit the uKnowKids site to see the latest offers available.



uknowkids
TESTIMONIALS & REVIEWS
OUR STORY
FEATURES & PRICING
PARENTING RESOURCES
SUPPORT & FAQS
LOG IN TO APP
SIGN UP

Keep your kids safe online and on the mobile phone with uKnowKids

Created by parents to help parents, uKnowKids is protecting kids in more than 90 countries around the world.

"Features such as monitoring apps, messages, and calls just aren't feasible on iOS—or so we thought. . . . [T]hrough its clever use of iCloud, [uKnowKids] offers monitoring functionality we didn't think was possible in an iPhone app. That makes [uKnowKids] our Editors' Choice for iPhone parental control apps."
-- PC Magazine, March 24, 2016

PC
PCMAG.COM
EDITORS' CHOICE

Start Your 1 Week FREE Trial Now!

Experience uKnowKids. Cancel Anytime

First Name
Last Name
Your Email Address
Password

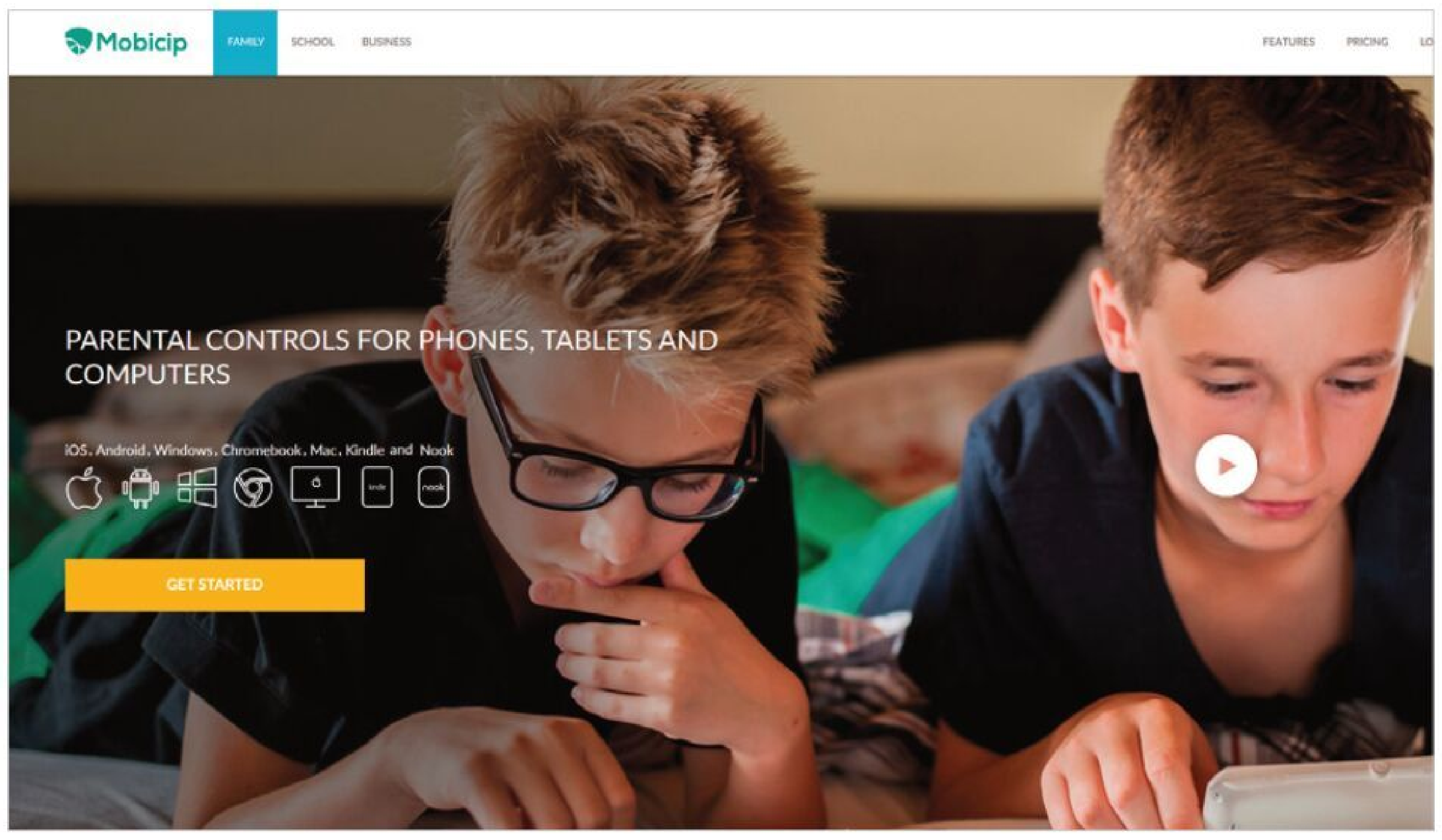
☐ I agree to all of the terms of the uKnowKids Terms of Service.

Protect My Kids Today

This is a 128-bit SSL Encrypted page and so your information will be securely transmitted.

MOBICIP

Mobicip is a cross-platform tool that offers app monitoring, web browsing monitoring, time limits and custom filters. The basic package is free but has some good features on offer, whilst the premium package costs $39.99 per year.



Mobicip
FAMILY
SCHOOL
BUSINESS
FEATURES
PRICING

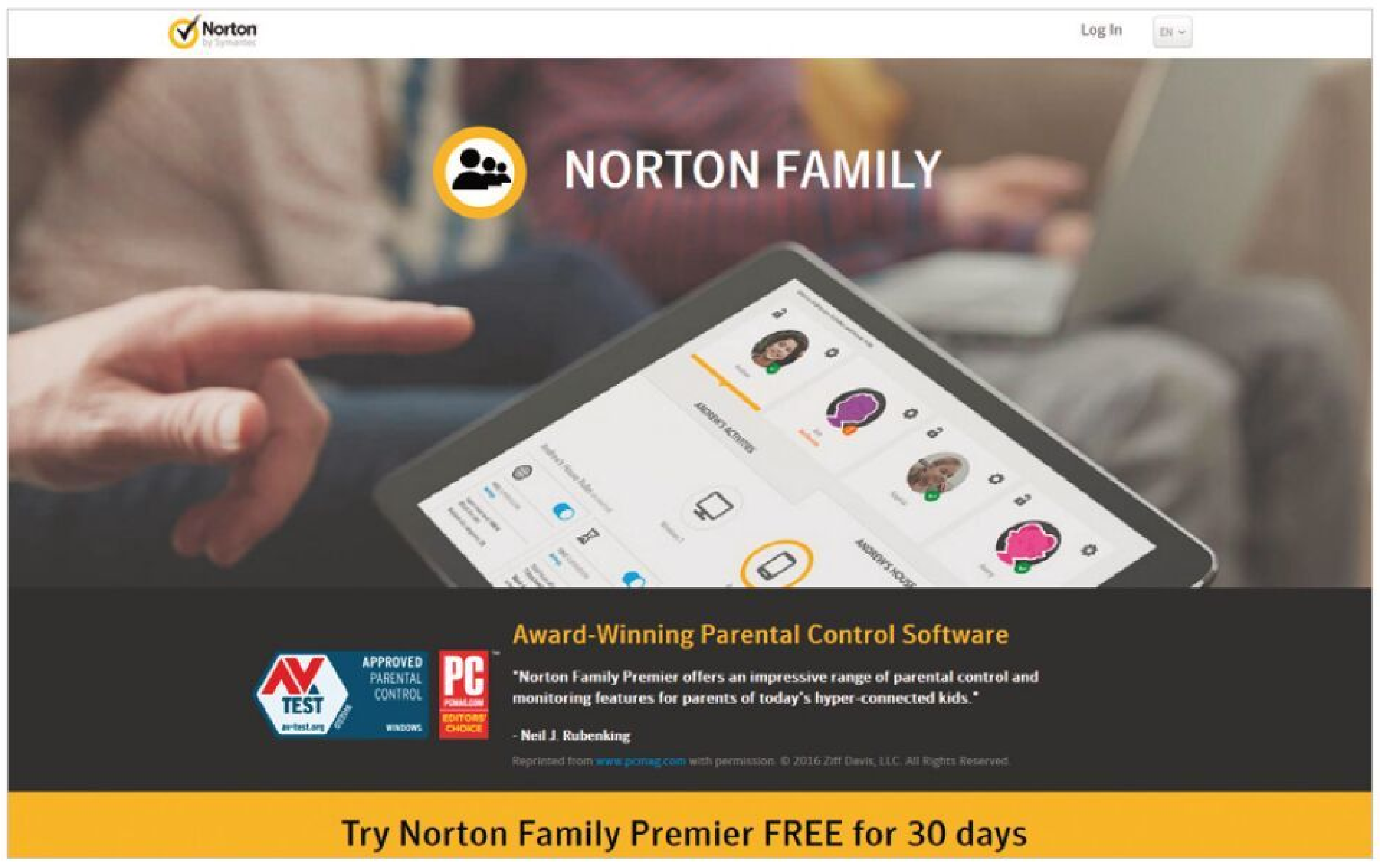
PARENTAL CONTROLS FOR PHONES, TABLETS AND COMPUTERS

iOS, Android, Windows, Chromebook, Mac, Kindle and Nook

GET STARTED

NORTON FAMILY

Norton Family is a previously mentioned tool that offers both free and paid for services to help protect children and young people online. It's cross-platform, provides protection for social media accounts, time supervision, activity monitoring and much more. Check the site for the latest features and pricing.



Norton
Log In
NORTON FAMILY
APPROVED PARENTAL CONTROL
AV TEST
av-test.org
WINDOWS
PC
PCMAG.COM
EDITORS' CHOICE

Award-Winning Parental Control Software

"Norton Family Premier offers an impressive range of parental control and monitoring features for parents of today's hyper-connected kids."

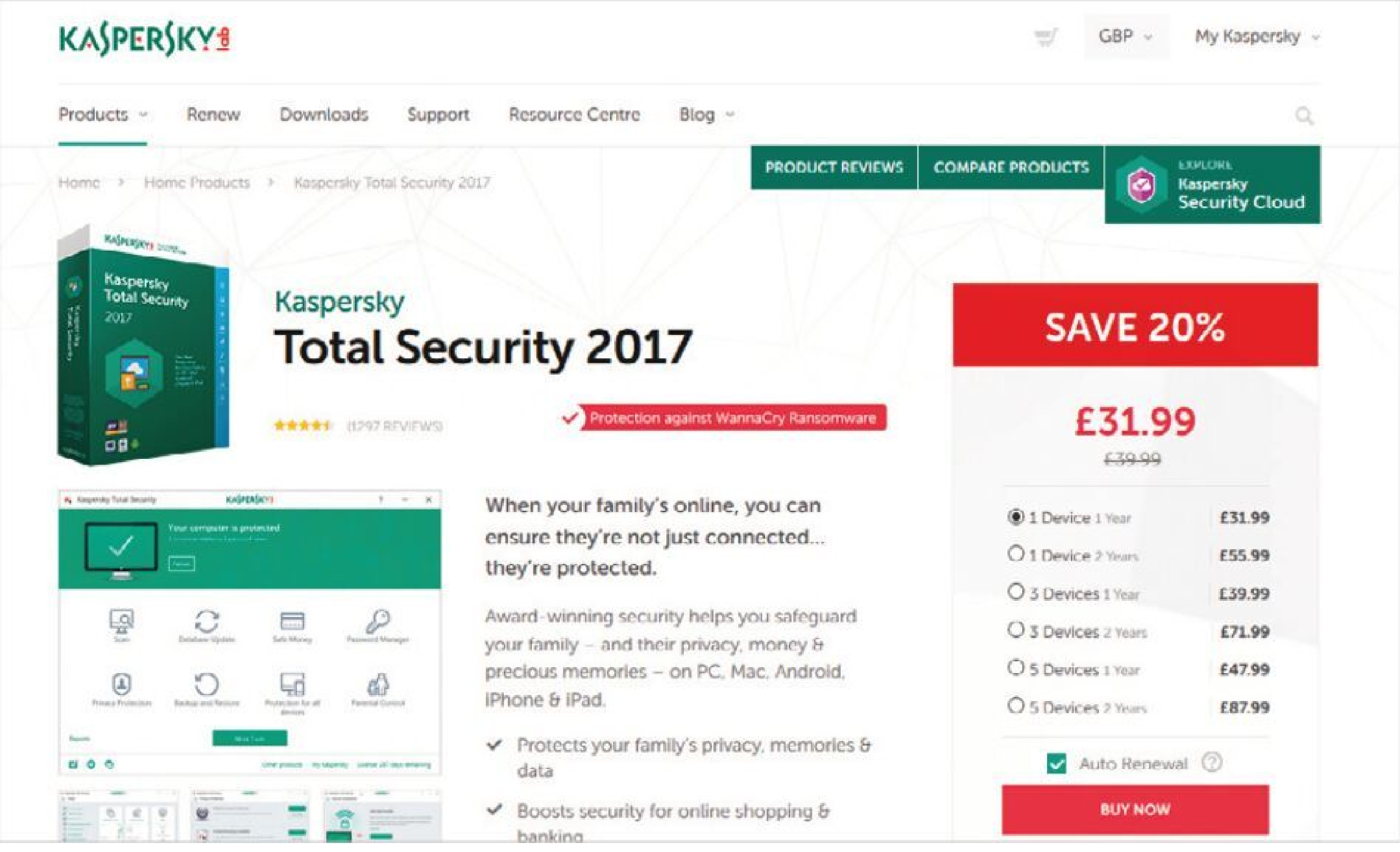
- Neil J. Rubenking

Reprinted from www.pcmag.com with permission. © 2016 Ziff Davis, LLC. All Rights Reserved.

Try Norton Family Premier FREE for 30 days

KASPERSKY

Kaspersky Total Security 2017/8, very much like Bitdefender, offers a parental control feature within its security suite. With it the parent or guardian can set time restrictions, block access to inappropriate content, monitor Internet activities and monitor communications on mobile devices. Prices start at just £31.99 per year for a single device.



KASPERSKY lab
GBP
My Kaspersky
Products
Renew
Downloads
Support
Resource Centre
Blog
Home > Home Products > Kaspersky Total Security 2017
PRODUCT REVIEWS
COMPARE PRODUCTS
EXPLORE Kaspersky Security Cloud
(1297 REVIEWS)
Protection against WannaCry Ransomware

Kaspersky
Total Security 2017

SAVE 20%

£31.99
~~£39.99~~

● 1 Device 1 Year	£31.99
○ 1 Device 2 Years	£55.99
○ 3 Devices 1 Year	£39.99
○ 3 Devices 2 Years	£71.99
○ 5 Devices 1 Year	£47.99
○ 5 Devices 2 Years	£87.99

☑ Auto Renewal

BUY NOW

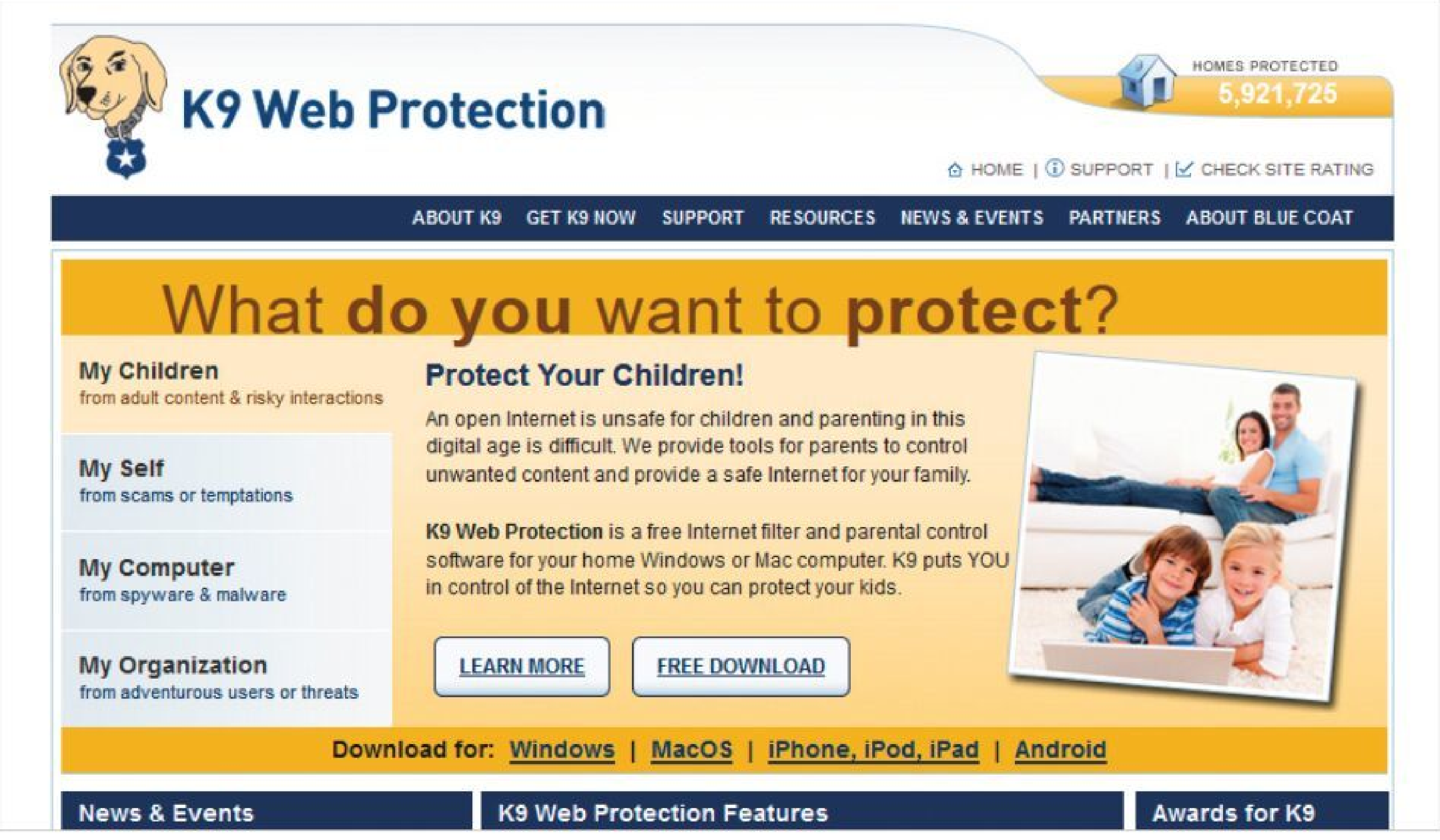
When your family's online, you can ensure they're not just connected... they're protected.

Award-winning security helps you safeguard your family – and their privacy, money & precious memories – on PC, Mac, Android, iPhone & iPad.

- ✓ Protects your family's privacy, memories & data
- ✓ Boosts security for online shopping & banking

K9 WEB PROTECTION

K9 Web Protection (nothing to do with protecting dogs from accessing the Internet) is a free, cloud-based Internet filter that blocks inappropriate content, sets time restrictions, forces safe search on all search engines and works on both Windows and Mac computers.



K9 Web Protection
HOMES PROTECTED
5,921,725
HOME | SUPPORT | CHECK SITE RATING
ABOUT K9
GET K9 NOW
SUPPORT
RESOURCES
NEWS & EVENTS
PARTNERS
ABOUT BLUE COAT

What **do you** want to **protect**?

My Children
from adult content & risky interactions

My Self
from scams or temptations

My Computer
from spyware & malware

My Organization
from adventurous users or threats

Protect Your Children!

An open Internet is unsafe for children and parenting in this digital age is difficult. We provide tools for parents to control unwanted content and provide a safe Internet for your family.

K9 Web Protection is a free Internet filter and parental control software for your home Windows or Mac computer. K9 puts YOU in control of the Internet so you can protect your kids.

LEARN MORE
FREE DOWNLOAD

Download for: Windows | MacOS | iPhone, iPod, iPad | Android

News & Events
K9 Web Protection Features
Awards for K9

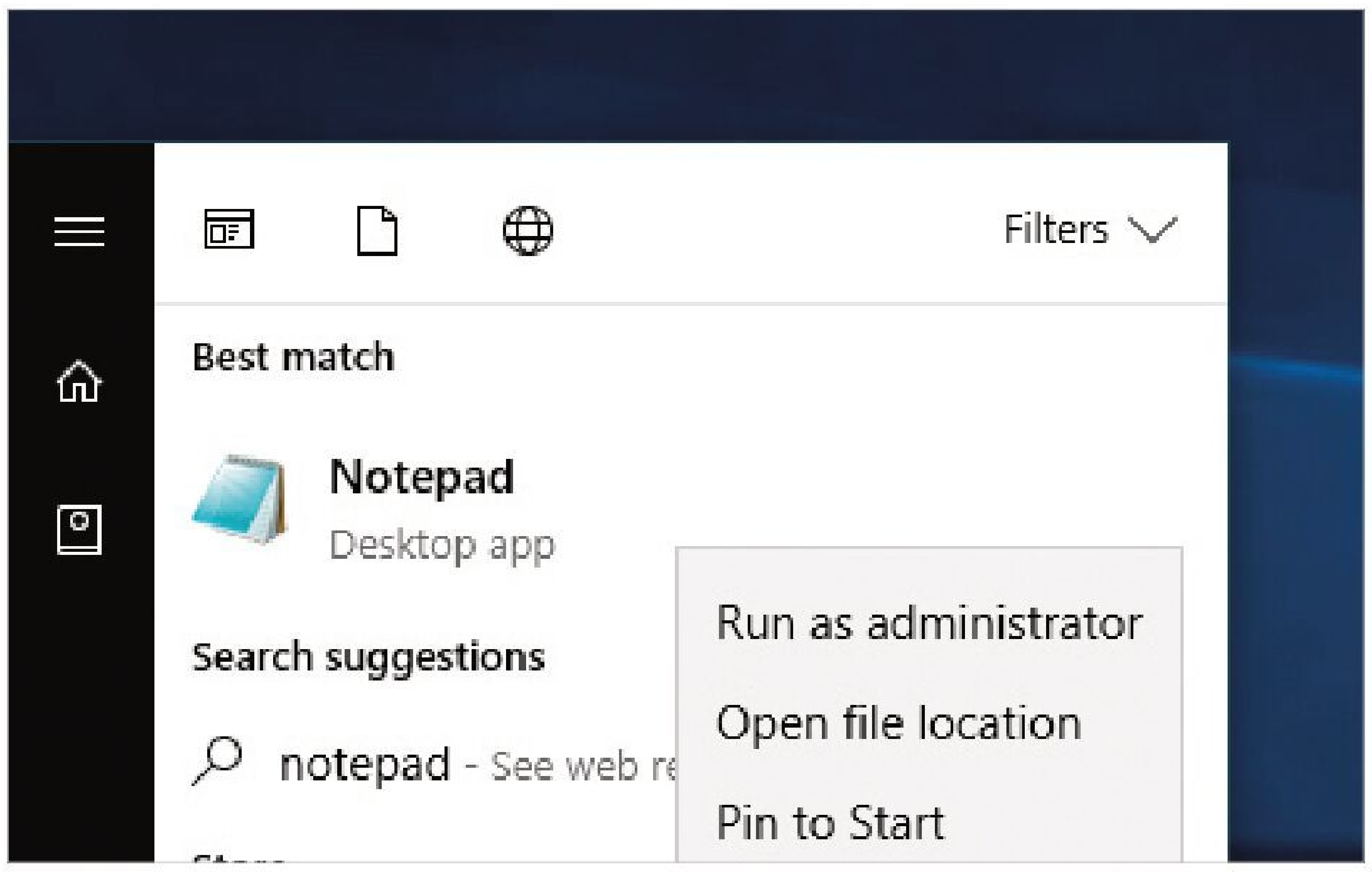
Using the Windows Hosts File to Block Sites

The Hosts file is used by the operating system to map hostnames to IP addresses. It's a historical file that's used by Windows to signpost internal and external websites, and other such networking services. You can use it to your advantage though.

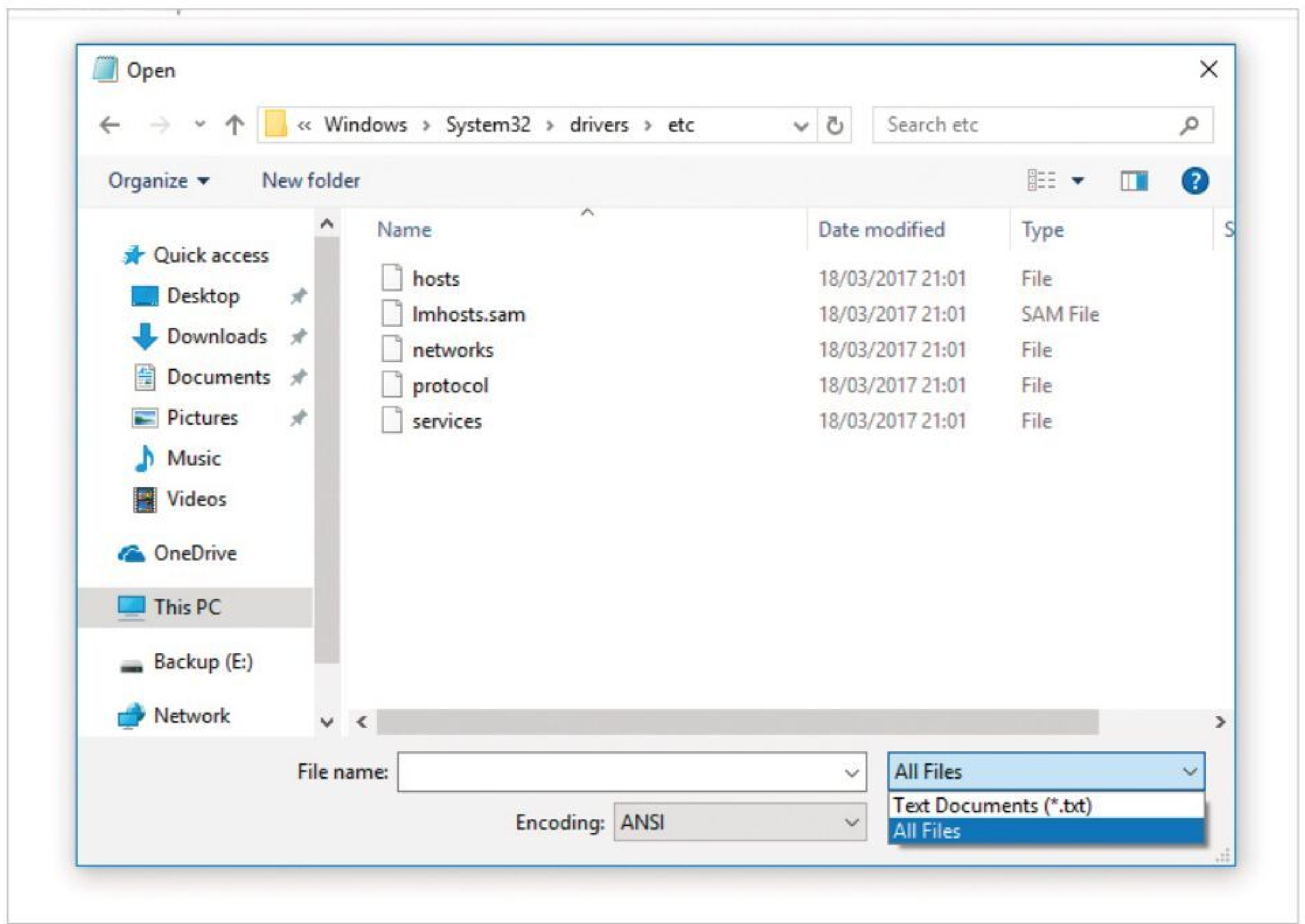
The Perfect Host

The Hosts file is simply a plain text file for mapping network locations and is checked by Windows to see if there's an entry whenever the user requests access to a website or network resource. Here's how to block websites using it.

STEP 1 First you need to open the Hosts file with administrative access. To do this, click on the Windows Start button and type notepad. When Notepad appears in the search list, right-click it and choose Run as Administrator from the menu and click Yes for the UAC message authentication.


Filters
Best match
Notepad
Desktop app
Search suggestions
notepad - See web re
Run as administrator
Open file location
Pin to Start

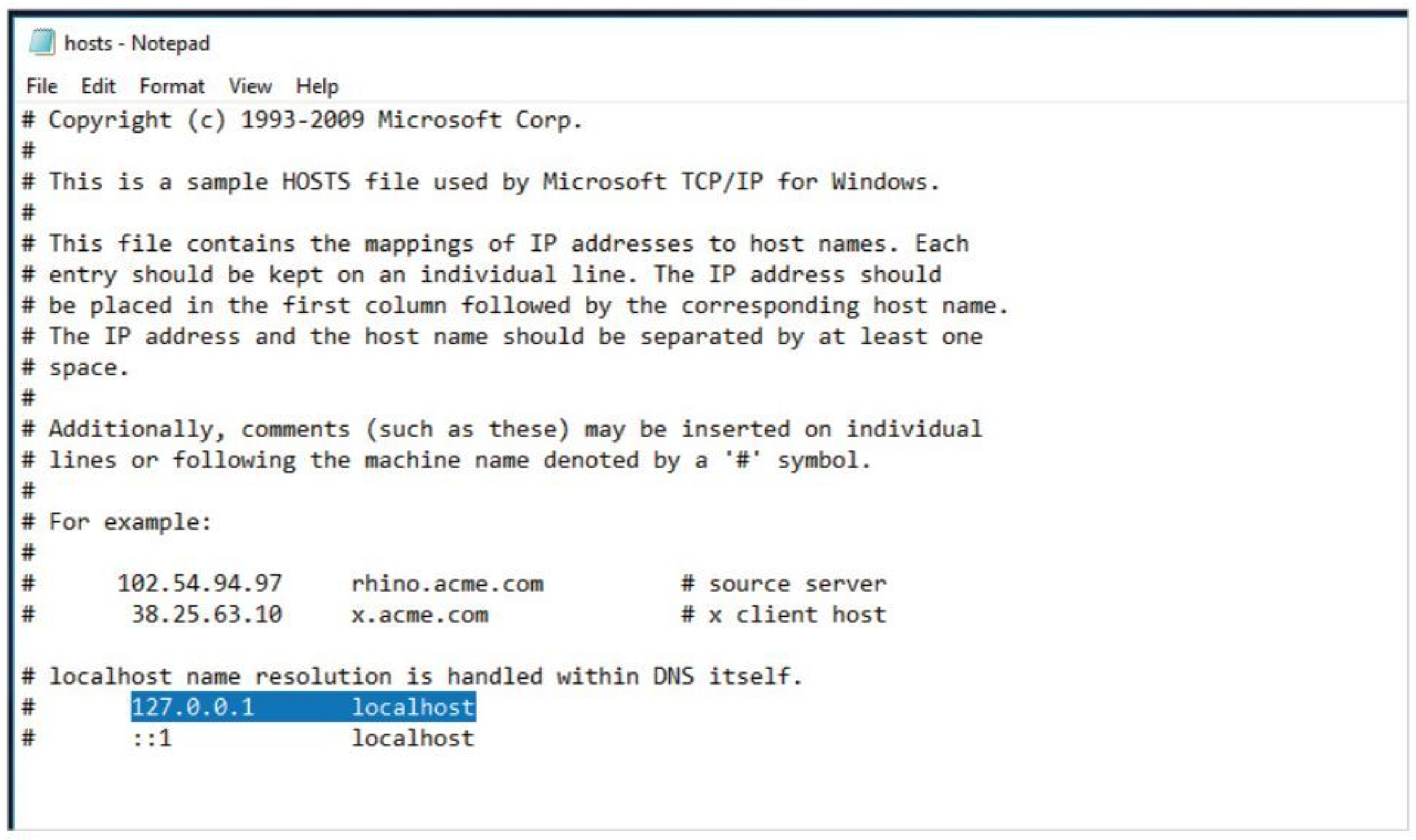
STEP 2 Within Notepad click File > Open and navigate to c:\Windows\System32\drivers\etc. Click the drop-down menu saying Text Documents and change it to All Files. This will list the files within the etc folder. Click on the Hosts file, then click the Open button.


Open
« Windows › System32 › drivers › etc
Search etc
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Backup (E:)
Network
Encoding: ANSI
Text Documents (*.txt)
All Files

Name	Date modified	Type
hosts	18/03/2017 21:01	File
lmhosts.sam	18/03/2017 21:01	SAM File
networks	18/03/2017 21:01	File
protocol	18/03/2017 21:01	File
services	18/03/2017 21:01	File

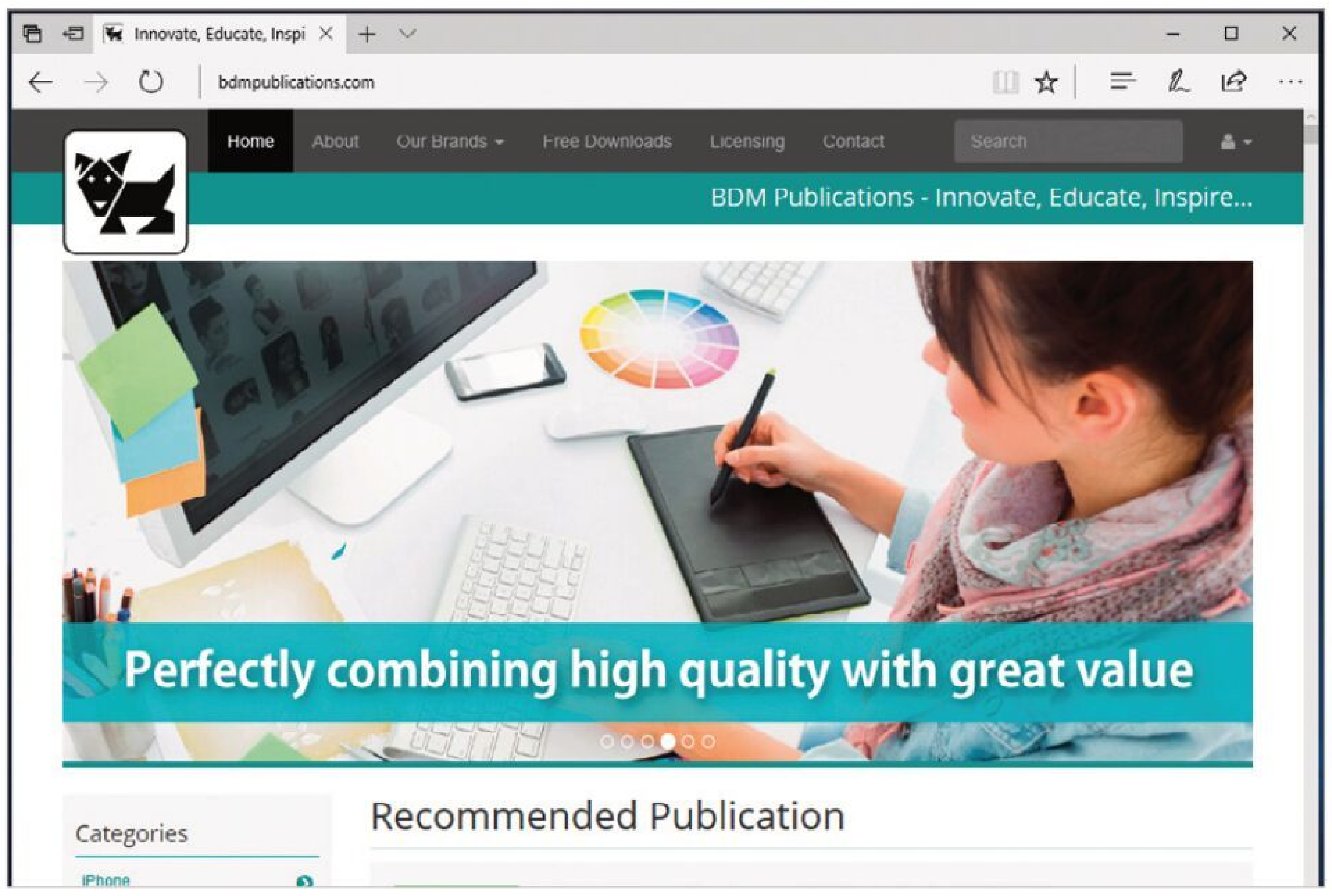
File name:
All Files

STEP 3 You can see that the Hosts file is a historic text file dating back from the early days of networking and communications. The localhost entry at the bottom of the file, 127.0.0.1 is your computer. This is the important entry, as we're going to fool the networking services into believing that a website is stored locally.

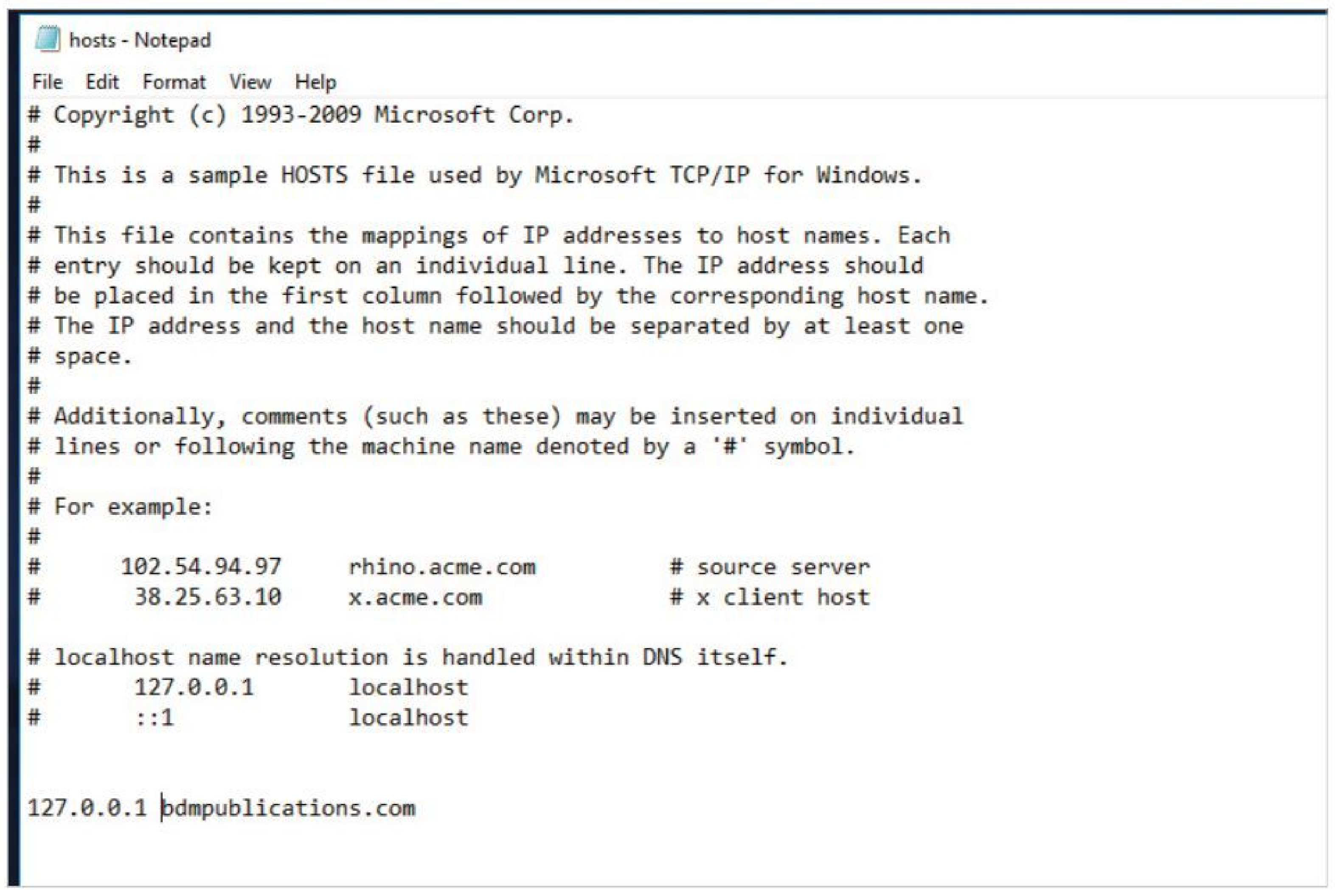

hosts - Notepad
File Edit Format View Help

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

STEP 4 It's this fooling Windows that makes this such an effective solution to blocking sites, as you're not fiddling with your router or other networking devices. Let's say, for example, you want to block BDM Publications. Open a browser and go to the BDM Publications website, **https://bdmpublications.com**.

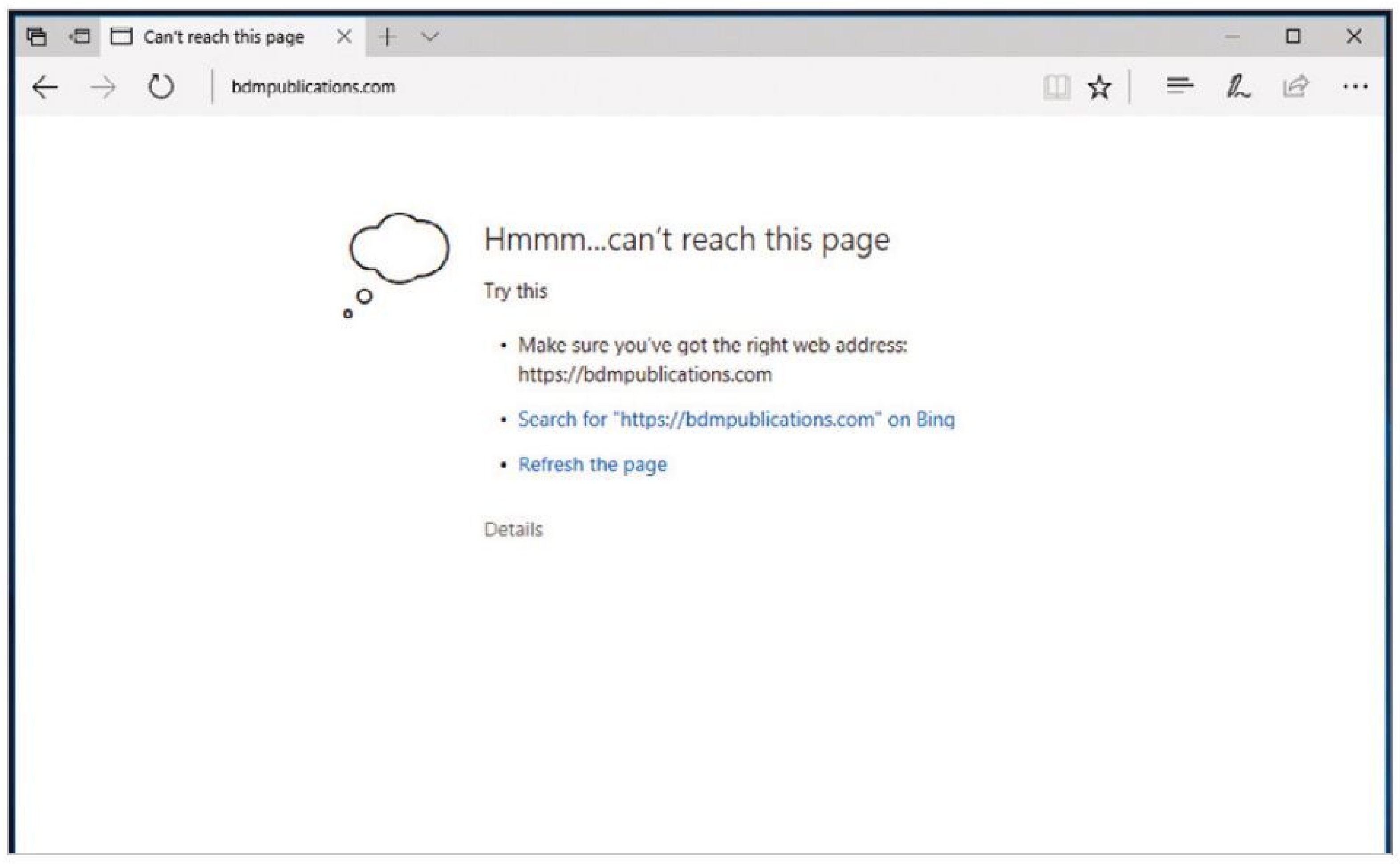

Innovate, Educate, Inspi
bdmpublications.com
Home
About
Our Brands
Free Downloads
Licensing
Contact
Search
BDM Publications - Innovate, Educate, Inspire...
Perfectly combining high quality with great value
Categories
iPhone
Recommended Publication

STEP 5 Either close or minimise the browser window and get back to the Hosts file in Notepad. Press Enter a couple of times to start a new line under the last hash and type in: **127.0.0.1 bdmpublications.com**. Don't add the HTTPS or the www part, just as it appears in the address bar.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


127.0.0.1 bdmpublications.com
```

STEP 6 In Notepad, click File > Save, to obviously save the newly edited Hosts file. Now get back to your browser and either refresh the page or close and reload the browser. When back up, in the address bar enter the site: **https://bdmpublications.com**. You can now see that the page won't load.



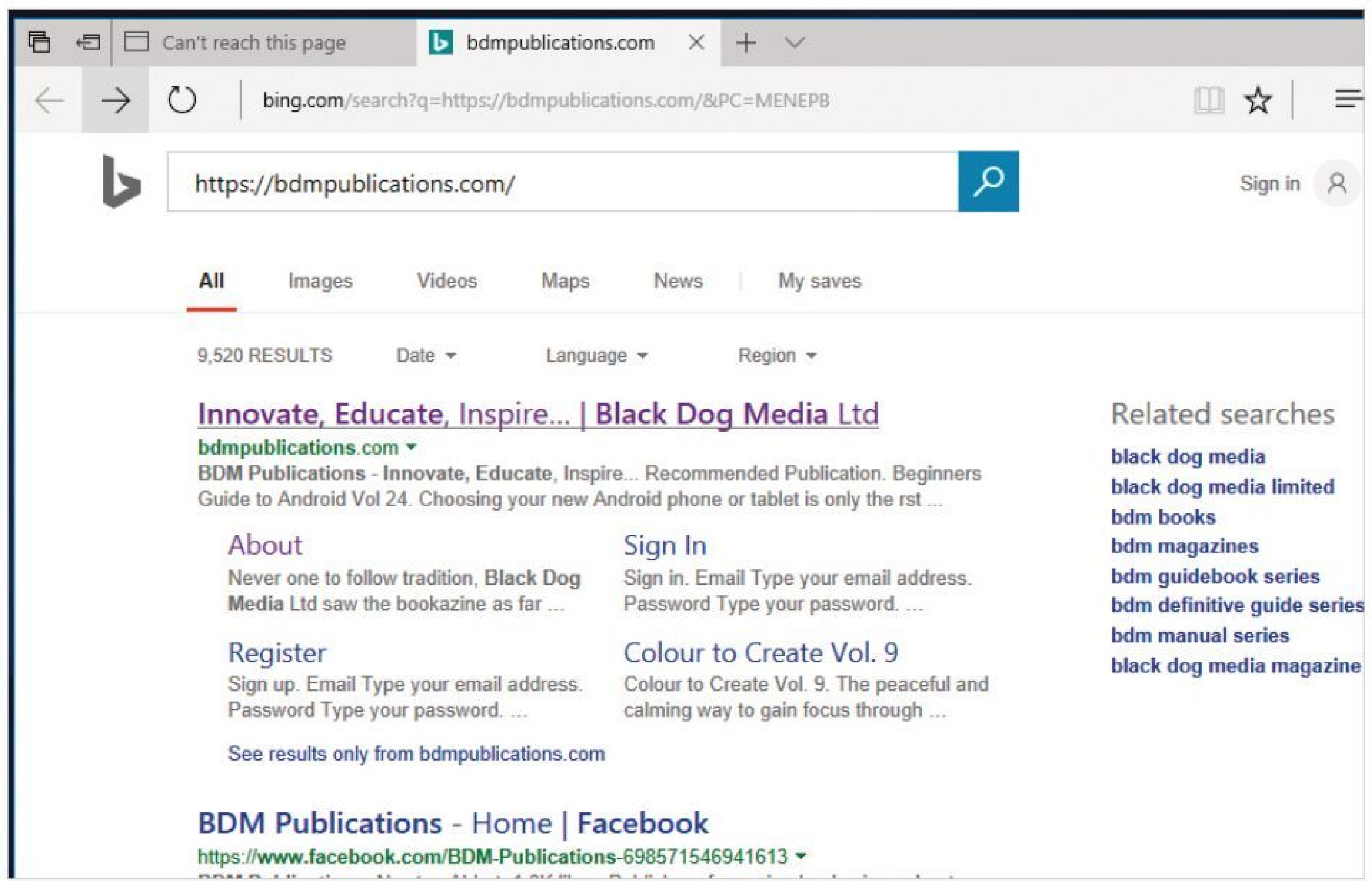
Hmmm...can't reach this page

Try this

- Make sure you've got the right web address: https://bdmpublications.com
- Search for "https://bdmpublications.com" on Bing
- Refresh the page

Details

STEP 7 You can try searching for it via Google or Bing but it still won't load as you've successfully blocked access to the website's hostname from the Hosts file. You can also see that any sub-domains after the main bdmpublications.com address are also blocked, which is certainly handy for some sites.



https://bdmpublications.com/

9,520 RESULTS

Innovate, Educate, Inspire... | Black Dog Media Ltd
bdmpublications.com
BDM Publications - Innovate, Educate, Inspire... Recommended Publication. Beginners Guide to Android Vol 24. Choosing your new Android phone or tablet is only the rst ...

About
Never one to follow tradition, Black Dog Media Ltd saw the bookazine as far ...

Sign In
Sign in. Email Type your email address. Password Type your password. ...

Register
Sign up. Email Type your email address. Password Type your password. ...

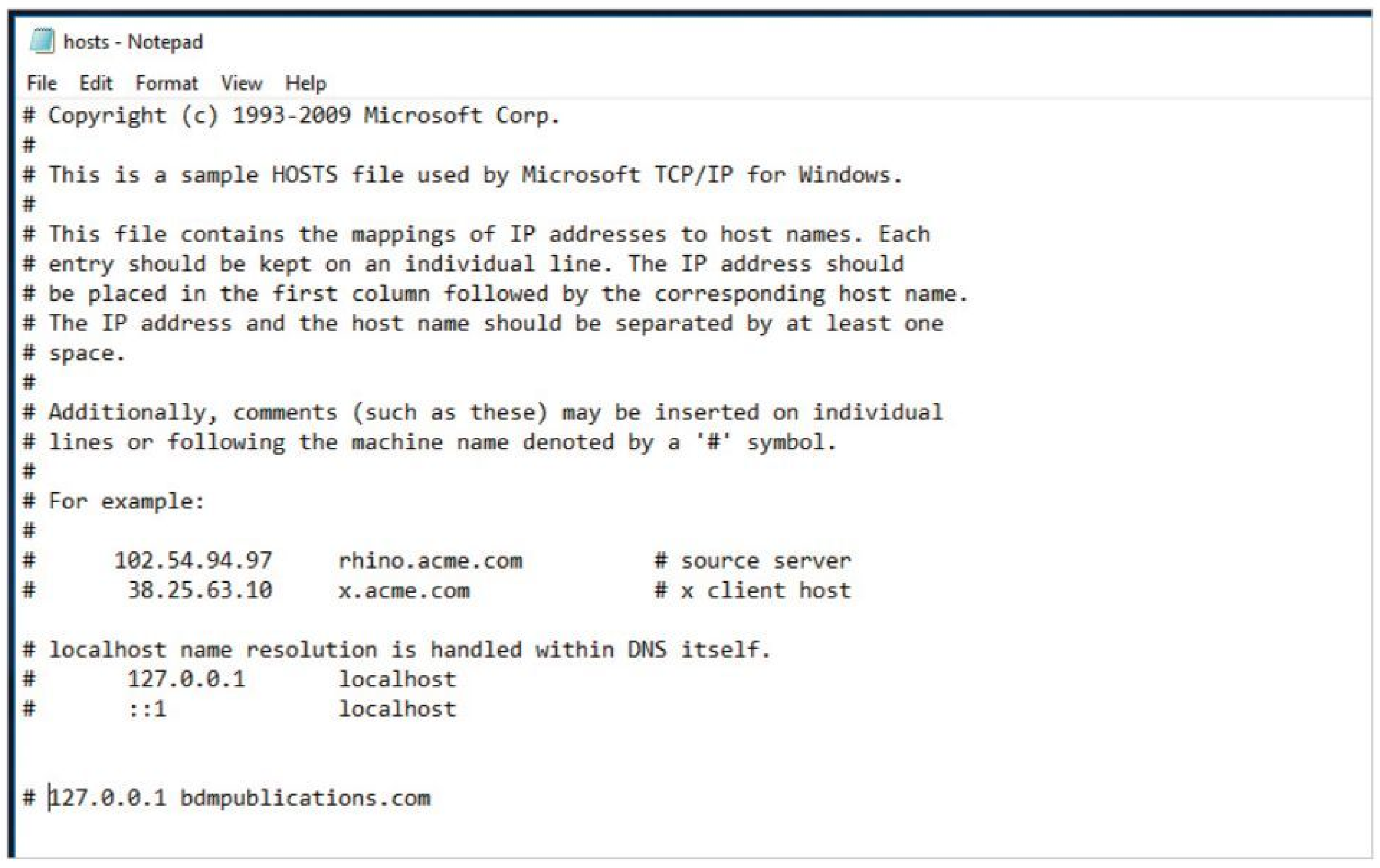
Colour to Create Vol. 9
Colour to Create Vol. 9. The peaceful and calming way to gain focus through ...

See results only from bdmpublications.com

BDM Publications - Home | Facebook
https://www.facebook.com/BDM-Publications-698571546941613

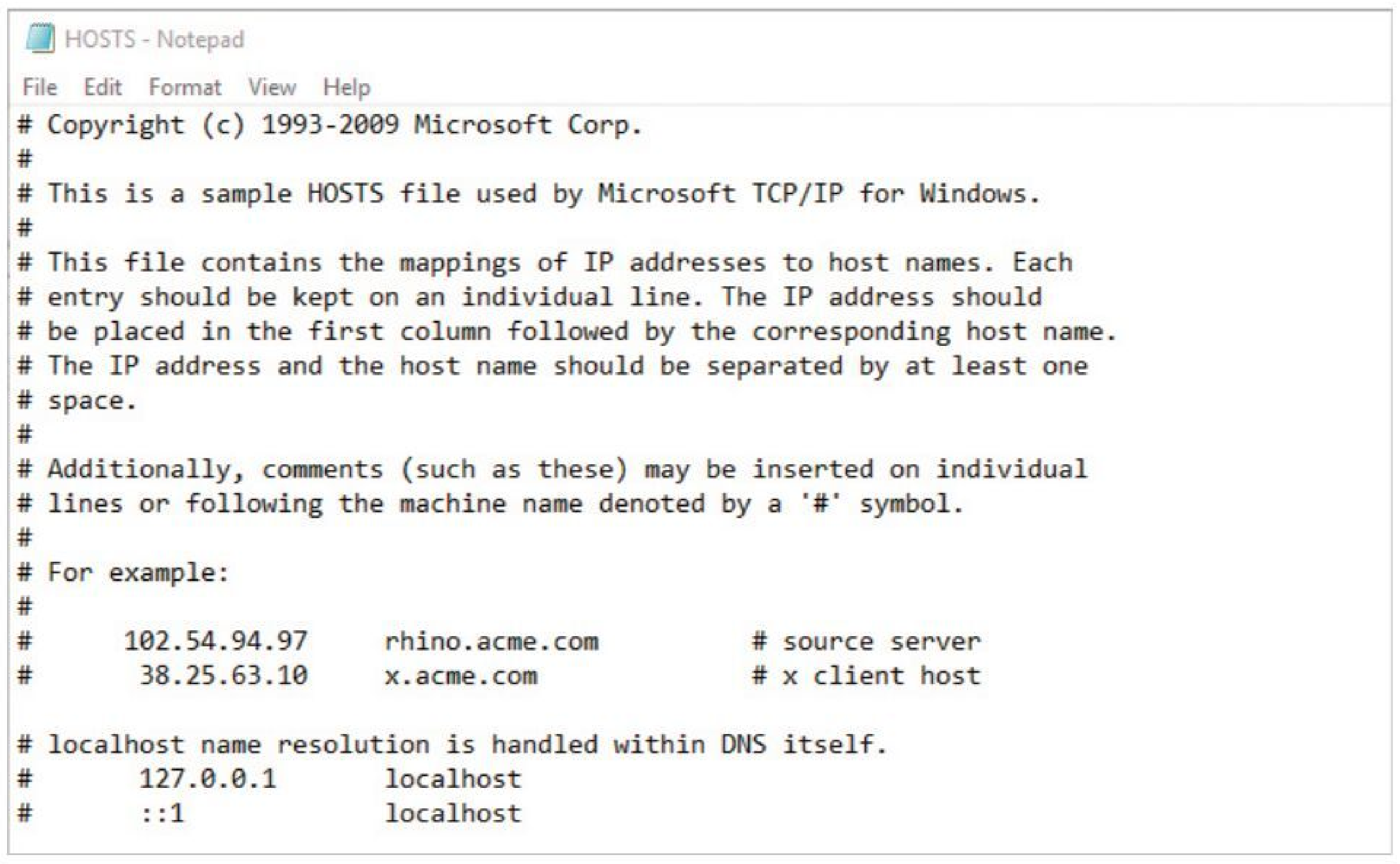
Related searches
black dog media
black dog media limited
bdm books
bdm magazines
bdm guidebook series
bdm definitive guide series
bdm manual series
black dog media magazine

STEP 8 What we've done here is fool Windows' networking services into thinking that the website bdmpublications.com, is being hosted on the computer itself and not out there on the Internet. If we wanted to remove the block, we can simply delete the line or put a hash at the start of the line and save the file.



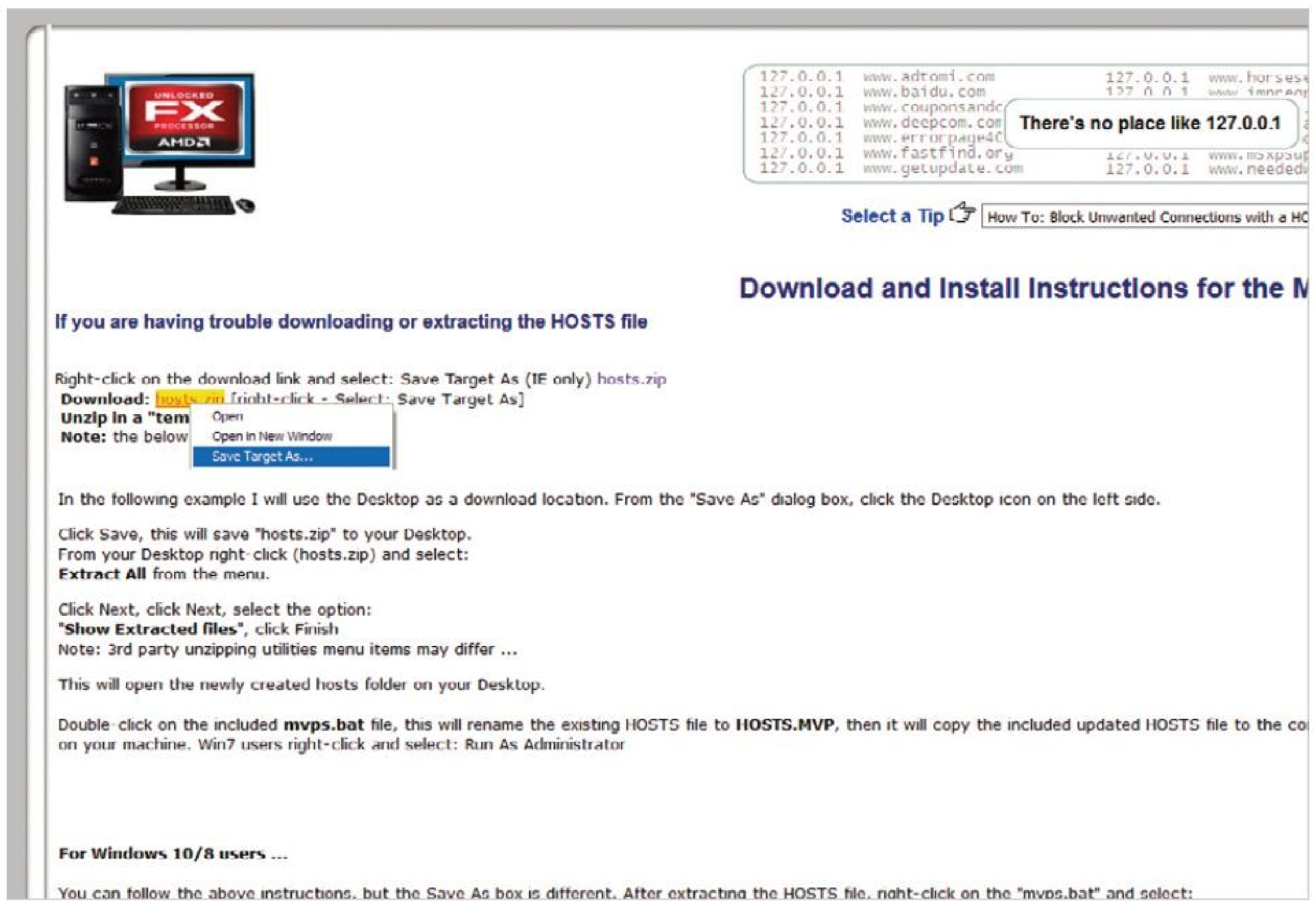
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


# 127.0.0.1 bdmpublications.com
```

STEP 9 Over time you can add more sites to the Hosts file list, pointing each one back to the 127.0.0.1 address of the local computer to block it from ever being reached; even if you use a different browser or other Internet accessible program.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

STEP 10 If you want a complete list that's already been created, then WinHelp2002 provides a downloadable compressed Hosts file that you can replace your own with. You can find it at **http://winhelp2002.mvps.org/hosts2.htm**; just read the instructions to replace the new Hosts file.


UNLOCKED
FX
PROCESSOR
AMD
There's no place like 127.0.0.1
Select a Tip
How To: Block Unwanted Connections with a HO
Open
Open in New Window
Save Target As...

```
127.0.0.1  www.adtomi.com        127.0.0.1  www.horses
127.0.0.1  www.baidu.com
127.0.0.1  www.couponsandc
127.0.0.1  www.deepcom.com
127.0.0.1  www.errorpage4C
127.0.0.1  www.fastfind.org
127.0.0.1  www.getupdate.com     127.0.0.1  www.needed
```

Download and Install Instructions for the M

If you are having trouble downloading or extracting the HOSTS file

Right-click on the download link and select: Save Target As (IE only) hosts.zip
Download: hosts.zip [right-click - Select: Save Target As]
Unzip in a "tem
Note: the below

In the following example I will use the Desktop as a download location. From the "Save As" dialog box, click the Desktop icon on the left side.

Click Save, this will save "hosts.zip" to your Desktop.
From your Desktop right-click (hosts.zip) and select:
Extract All from the menu.

Click Next, click Next, select the option:
"Show Extracted files", click Finish
Note: 3rd party unzipping utilities menu items may differ ...

This will open the newly created hosts folder on your Desktop.

Double-click on the included **mvps.bat** file, this will rename the existing HOSTS file to **HOSTS.MVP**, then it will copy the included updated HOSTS file to the co on your machine. Win7 users right-click and select: Run As Administrator

For Windows 10/8 users ...

You can follow the above instructions, but the Save As box is different. After extracting the HOSTS file, right-click on the "mvps.bat" and select:

Further Protection for Young Adults

Younger children are certainly vulnerable when on the Internet but from 13-years a teenager is allowed to have a Facebook, Twitter and other social media accounts. This opens up a whole new level of online protection issues and significant dangers within.

We look at how you can help protect their social media status and how to create their own Windows accounts.

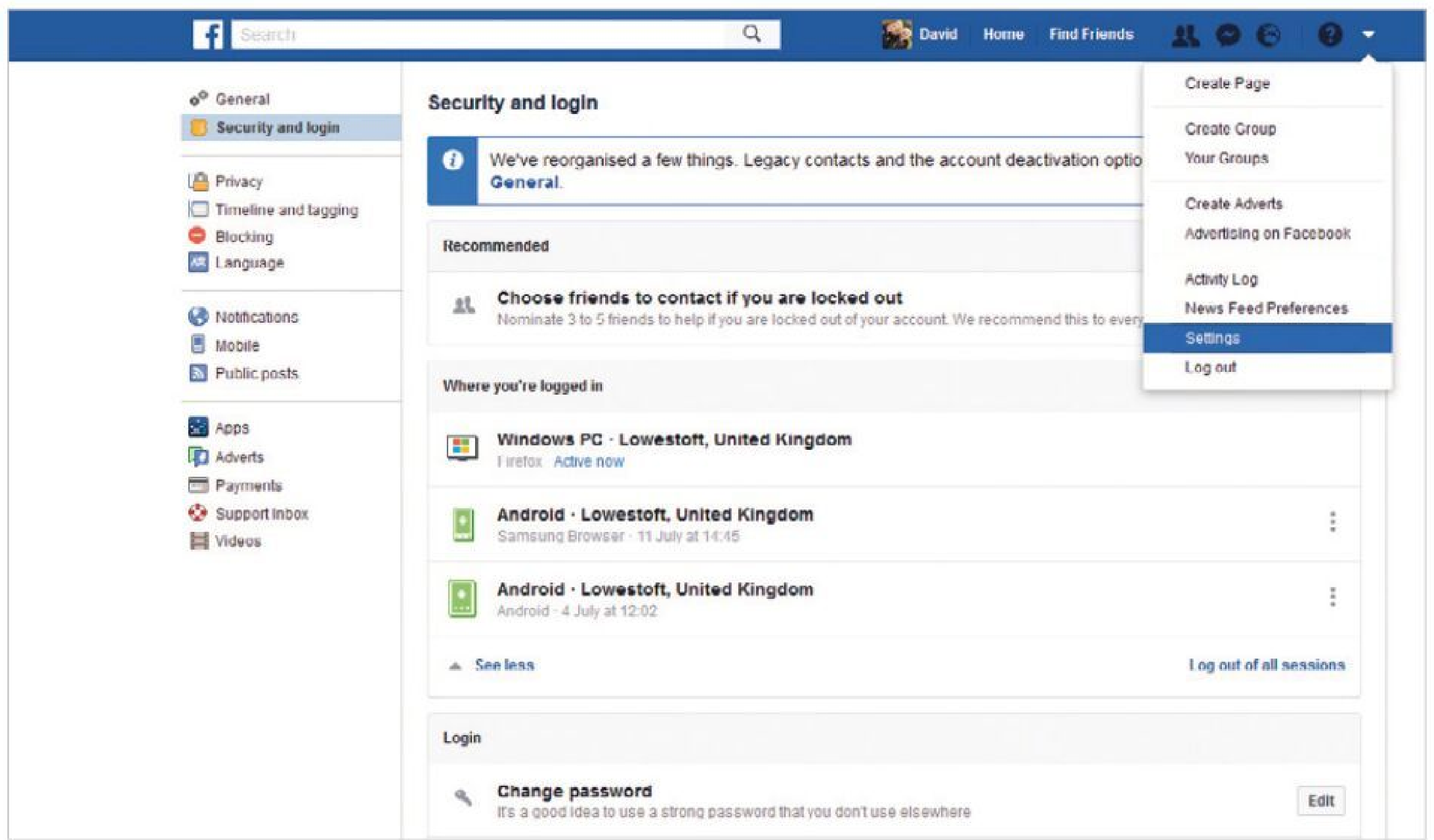
Staying Safe with Facebook for Teens

If your child is thirteen they're now, according to the rules of the company, allowed to have a Facebook account. Facebook's popularity has waned in recent years with teens but it's still heavily used. Therefore, we need to make sure that our teens are safe when on it.

Smells Like Teen Facebook

Providing you adhere to the recommended security settings for Facebook, and don't add just anyone who sends you a friend request, you should be relatively safe. However, these ten tips will help.

Get to the Facebook security settings by clicking on the Down Arrow next to the question mark in the top right of the Facebook interface. From there click the Settings option on the menu and then Security and login on the left-hand panel. If you haven't already, make sure you're using a strong password, as suggested earlier in this book.


Search
David
Home
Find Friends
Create Page
Create Group
Your Groups
Create Adverts
Advertising on Facebook
Activity Log
News Feed Preferences
Settings
Log out
General
Security and login
Privacy
Timeline and tagging
Blocking
Language
Notifications
Mobile
Public posts
Apps
Adverts
Payments
Support Inbox
Videos
See less
Log out of all sessions
Edit

Security and login

We've reorganised a few things. Legacy contacts and the account deactivation optio
General.

Recommended

Choose friends to contact if you are locked out
Nominate 3 to 5 friends to help if you are locked out of your account. We recommend this to every

Where you're logged in

Windows PC · Lowestoft, United Kingdom
Firefox · Active now

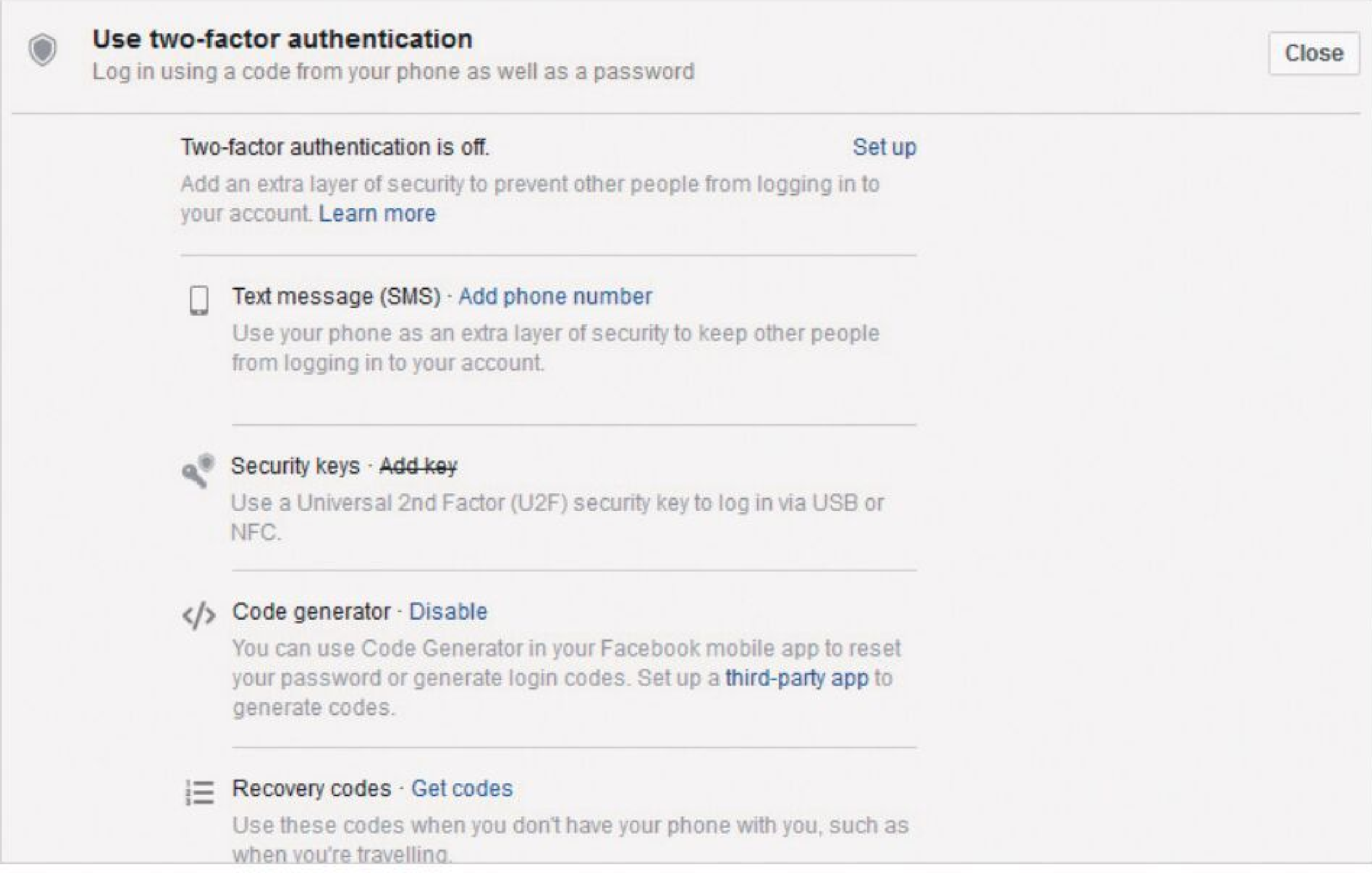
Android · Lowestoft, United Kingdom
Samsung Browser · 11 July at 14:45

Android · Lowestoft, United Kingdom
Android · 4 July at 12:02

Login

Change password
It's a good idea to use a strong password that you don't use elsewhere

In the same section, you're also able to set up two-factor authentication, utilising your phone, where Facebook will send a code to login with along with using your password. This elevated level of security ensures a higher degree of safety, as your account will be extremely difficult to hack.


Close
Set up
Learn more
Add phone number
Disable
third-party app
Get codes

Use two-factor authentication
Log in using a code from your phone as well as a password

Two-factor authentication is off.
Add an extra layer of security to prevent other people from logging in to your account. Learn more

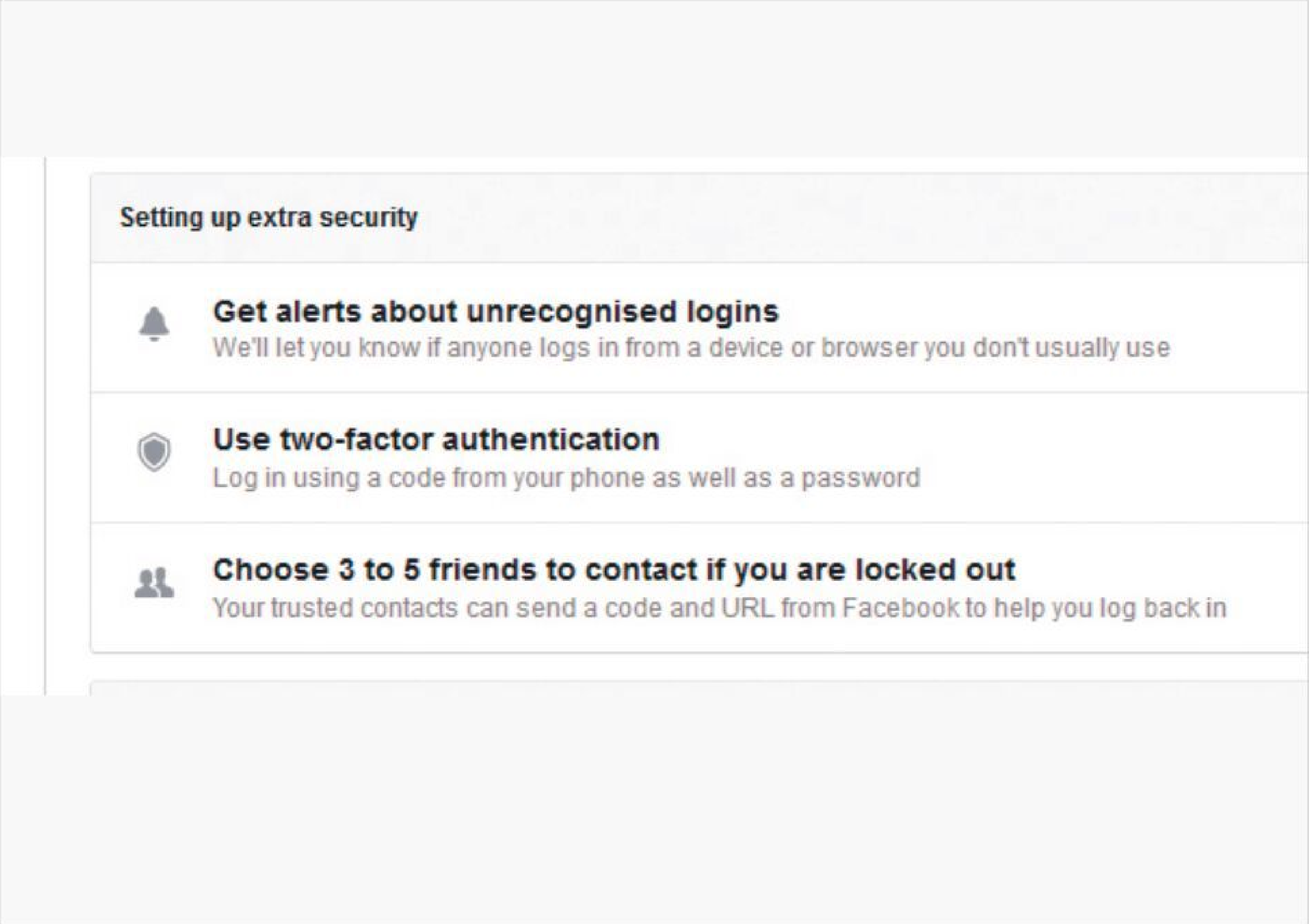
Text message (SMS) · Add phone number
Use your phone as an extra layer of security to keep other people from logging in to your account.

Security keys · ~~Add key~~
Use a Universal 2nd Factor (U2F) security key to log in via USB or NFC.

Code generator · Disable
You can use Code Generator in your Facebook mobile app to reset your password or generate login codes. Set up a third-party app to generate codes.

Recovery codes · Get codes
Use these codes when you don't have your phone with you, such as when you're travelling.

Whilst in the Security and login page, click the 'Get alerts about unrecognised logins' section's Edit box, this enables you to view if your account is logged in from an unrecognised device. This particular function is handy to keep track of when and where your Facebook account is being used.



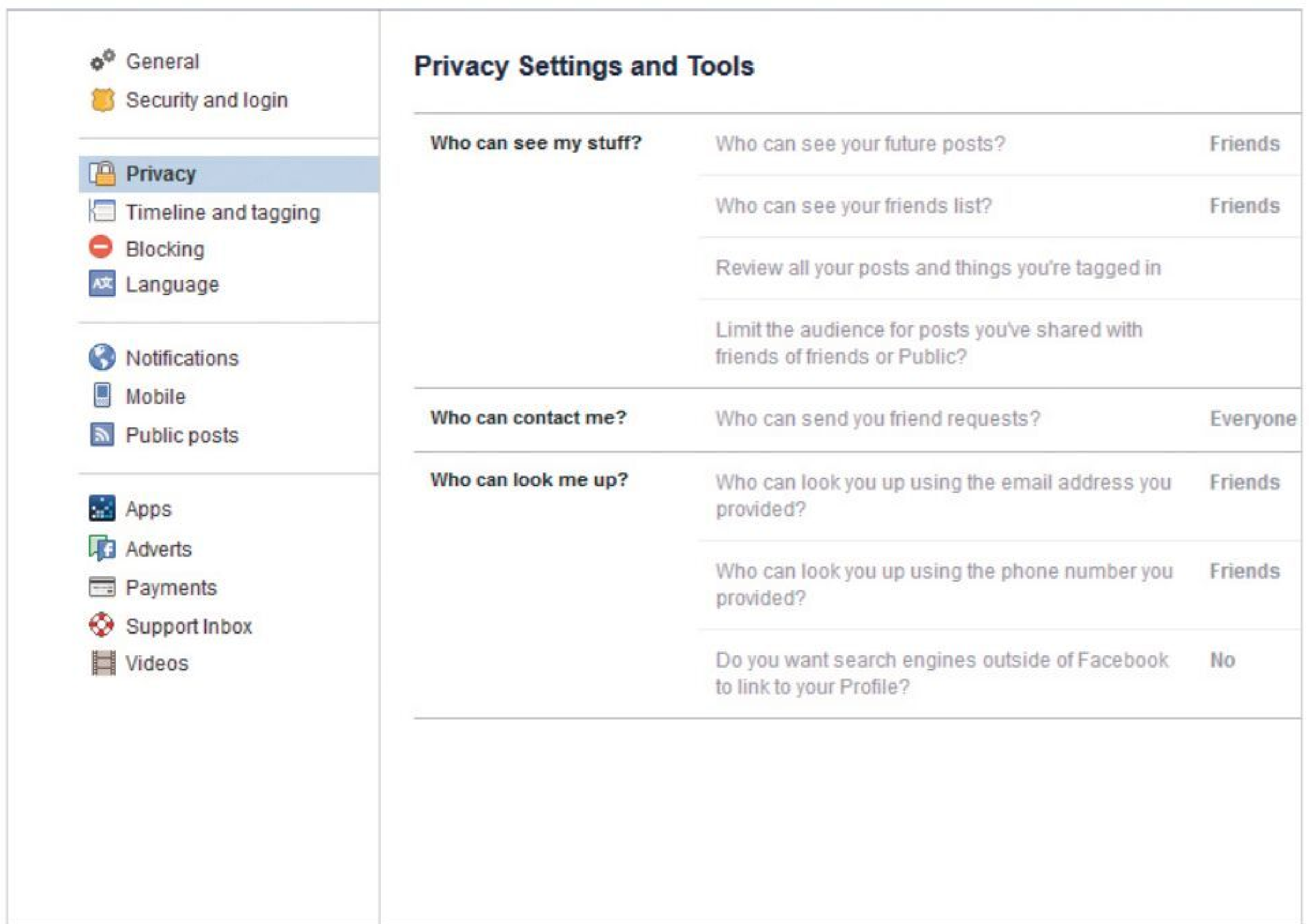
Setting up extra security

Get alerts about unrecognised logins
We'll let you know if anyone logs in from a device or browser you don't usually use

Use two-factor authentication
Log in using a code from your phone as well as a password

Choose 3 to 5 friends to contact if you are locked out
Your trusted contacts can send a code and URL from Facebook to help you log back in

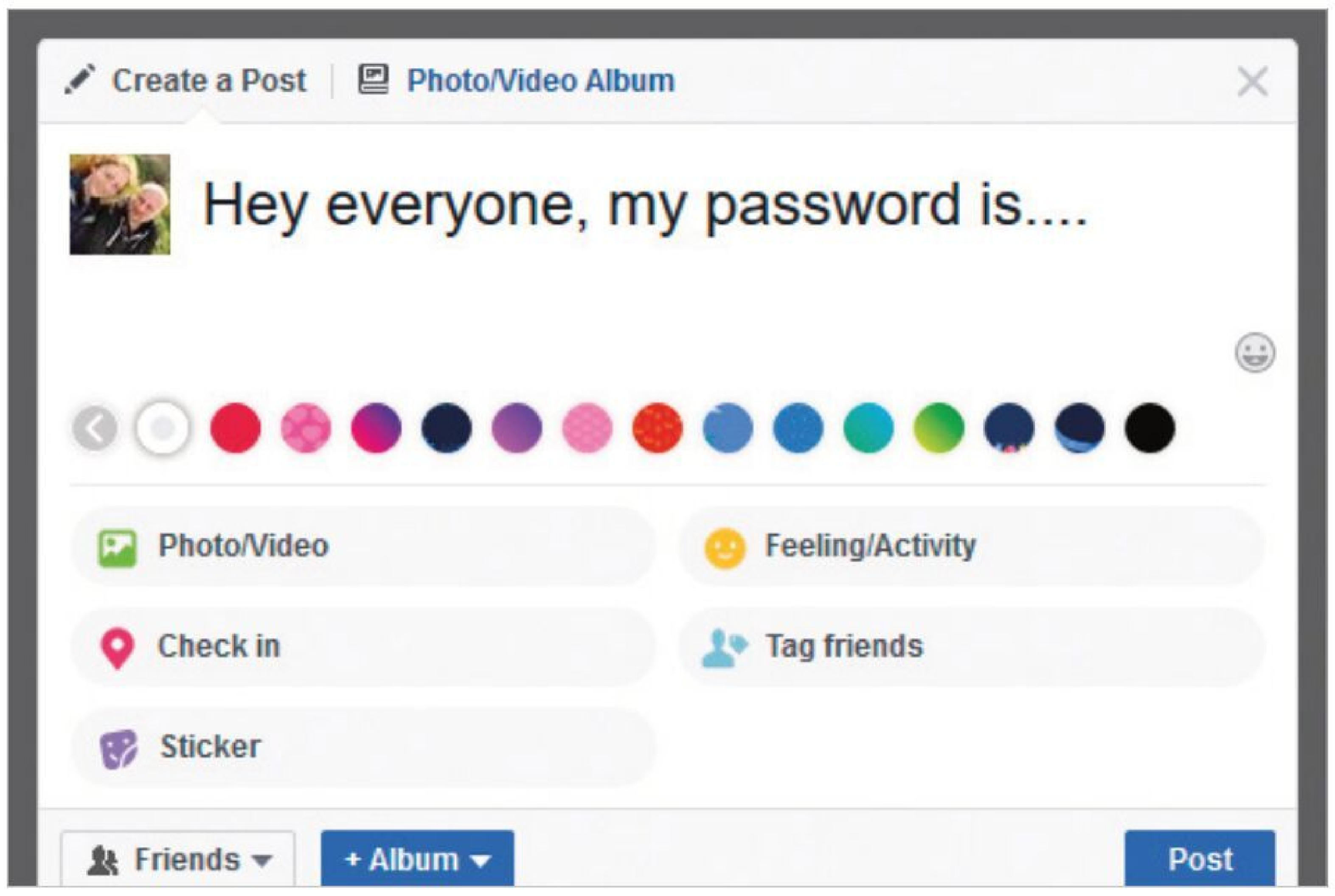
Click on the next section heading on the left-hand pane, Privacy. Take a moment to run through each of the options in this page, to ensure that your account is as private as possible, whilst still being available for true friends and family to add you to their friends lists.


General
Security and login
Privacy
Timeline and tagging
Blocking
Language
Notifications
Mobile
Public posts
Apps
Adverts
Payments
Support Inbox
Videos

Privacy Settings and Tools

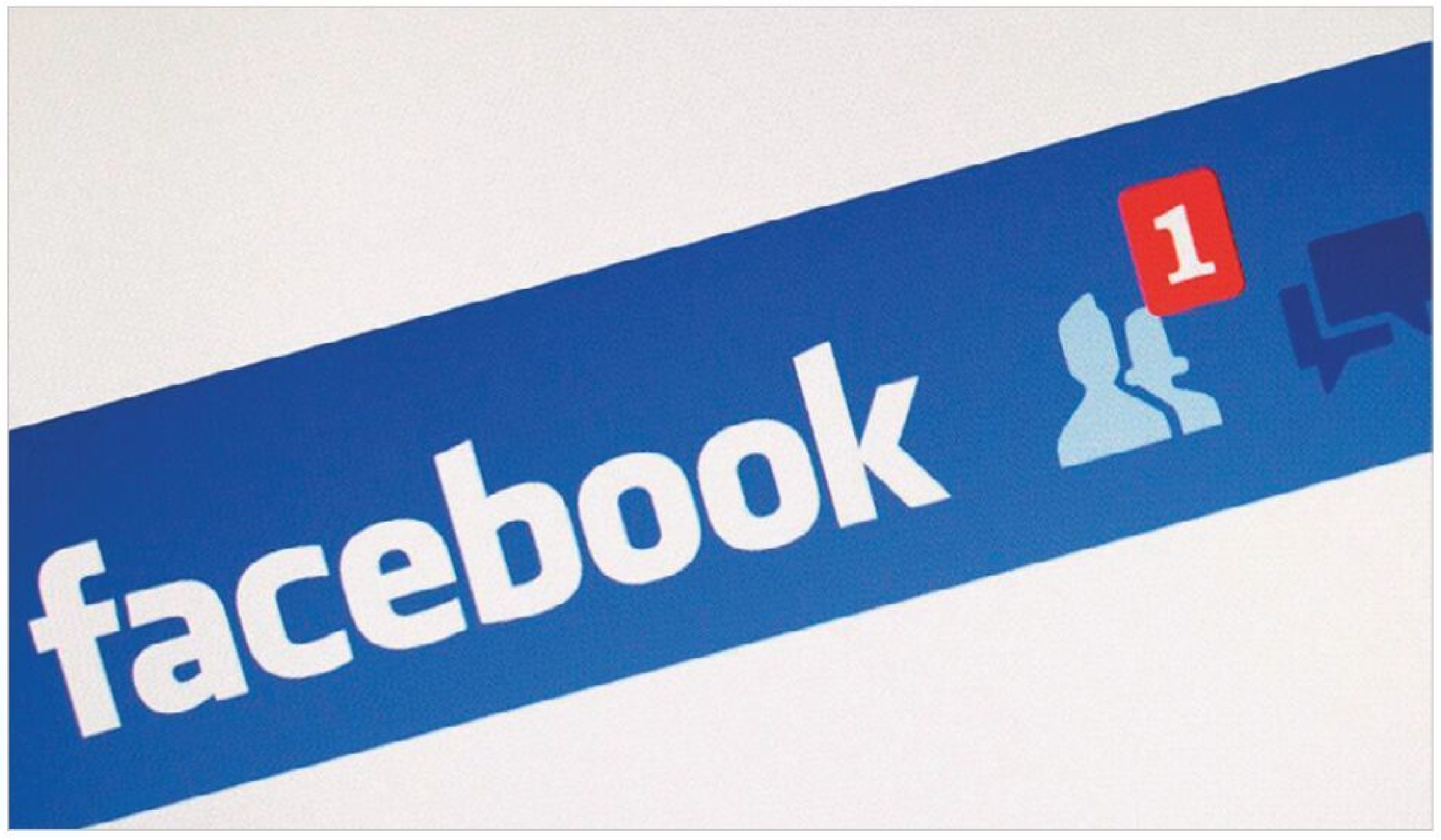
Who can see my stuff?	Who can see your future posts?	Friends
	Who can see your friends list?	Friends
	Review all your posts and things you're tagged in	
	Limit the audience for posts you've shared with friends of friends or Public?	
Who can contact me?	Who can send you friend requests?	Everyone
Who can look me up?	Who can look you up using the email address you provided?	Friends
	Who can look you up using the phone number you provided?	Friends
	Do you want search engines outside of Facebook to link to your Profile?	No

We're sure you don't need telling this, but never type your password into your Timeline. It may sound like a very basic tip but there have been instances of users being fooled, or simply not thinking of what they're doing or where they're typing, into entering their password into the Facebook Timeline.

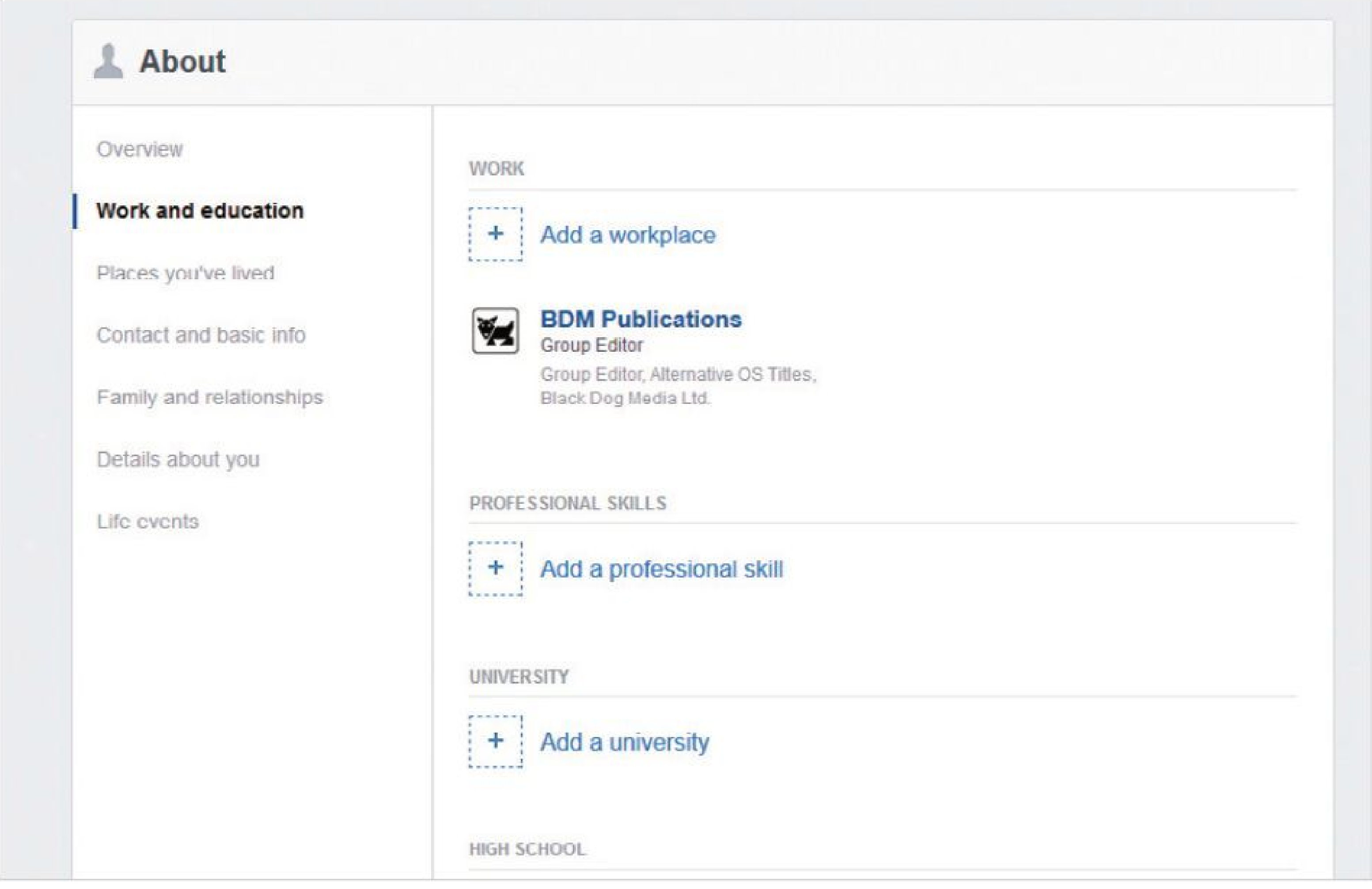

Create a Post
Photo/Video Album
Photo/Video
Feeling/Activity
Check in
Tag friends
Sticker
Friends
+ Album
Post

Hey everyone, my password is....

Never accept a friend request from a random stranger. Sometimes they accompany their request with a message, something along the lines of 'hey, remember me? We met in town…', or something similar. The hope is that you'll accept the request blindly and once in your friend list, they can get all manner of details from you.



Although it's nice to put forward information about yourself in your Facebook account, be a little cautious and consider not entering too many details. It's very easy for someone to then retrieve information regarding your date of birth, where you live, where you went to school, where you work and so on.

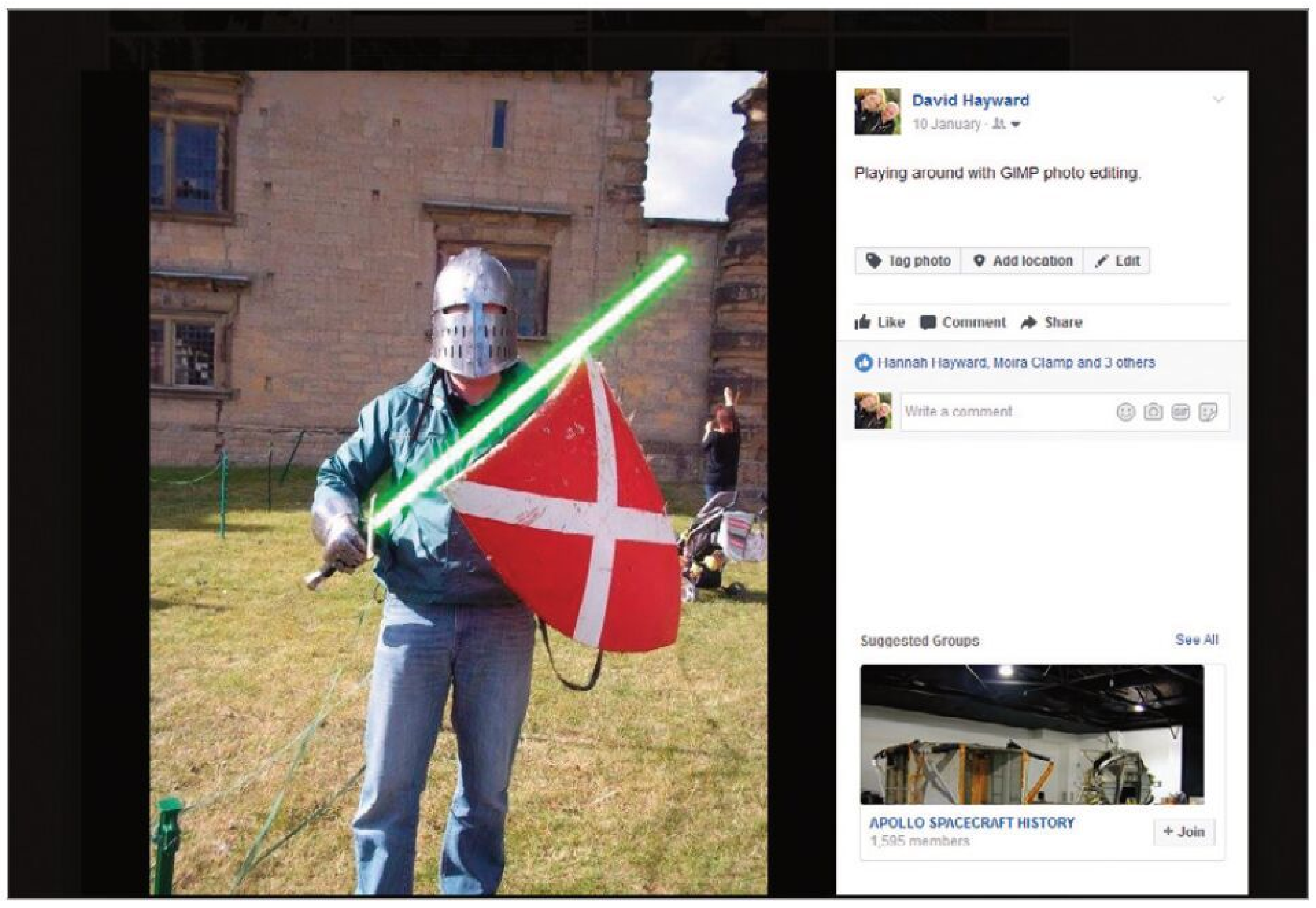

About
Overview
Work and education
Places you've lived
Contact and basic info
Family and relationships
Details about you
Life events
WORK
Add a workplace
PROFESSIONAL SKILLS
Add a professional skill
UNIVERSITY
Add a university
HIGH SCHOOL

BDM Publications
Group Editor
Group Editor, Alternative OS Titles, Black Dog Media Ltd.

Try to avoid being drawn into mass phishing posts, where the response asking is along the lines of 'List five things about yourself, then pass it on', or even posts that ask for likes. These are generated to catch active user accounts, which can then be used for phishing attempts.

Don't be fooled into thinking that posts asking for people to help locate a missing child, pet or object are real. Not only are most of these phishing attempts but often they can be attempts of someone trying to find a person; there could be a reason that the person in question has left, an abusive relationship perhaps.

Always think before you enter a post or reply to one. Just as you would in life, sometimes it's best not to say anything at all rather than offend or anger someone who's is blatantly baiting others. Think also about what images you post. Could your address or other details be discovered from the image?


Tag photo
Add location
Edit
Like
Comment
Share
Write a comment
Suggested Groups
See All
+ Join

David Hayward
10 January

Playing around with GIMP photo editing.

Hannah Hayward, Moira Clamp and 3 others

APOLLO SPACECRAFT HISTORY
1,595 members

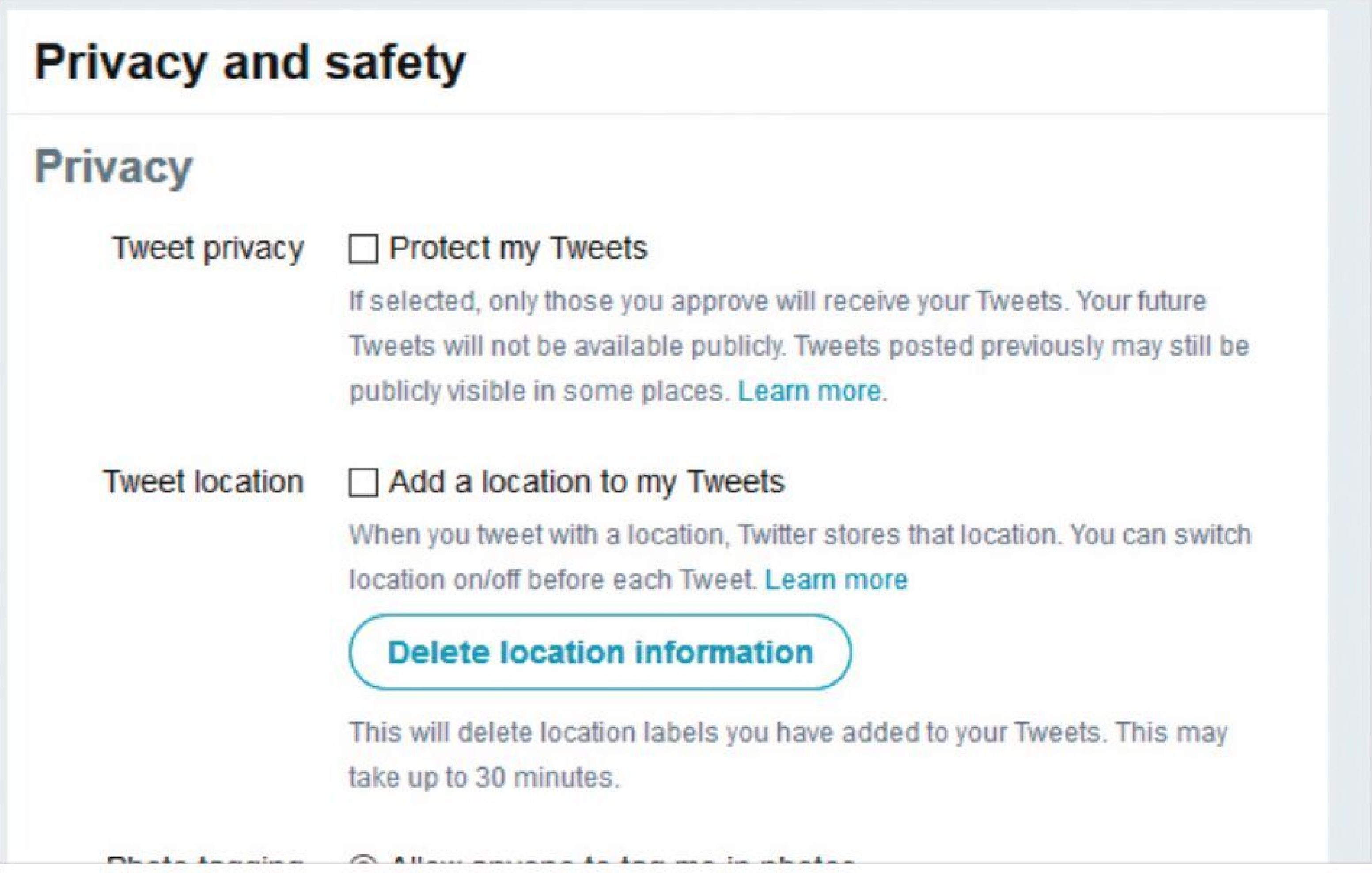
Staying Safe with Twitter for Teens

Twitter has been seen as both a force for good, allowing users from other parts of the world to communicate with what's going on in their country and as a platform for the nastier side of humanity. For teens, there's a lot to consider with staying safe on Twitter.

Twitter Twits

The age for setting up a Twitter account is thirteen but even adults can find themselves in a pickle from an errant Tweet or a Twitter-based phishing scam. Here are ten tips to help keep you safe on Twitter.

In Twitter, click on your profile picture and choose Settings and Privacy from the menu. To the left-side of the Twitter interface, click on the Privacy and safety link. Consider enabling Tweet Privacy and disabling Discoverability for improved safety.



Privacy and safety

Privacy

Tweet privacy ☐ Protect my Tweets

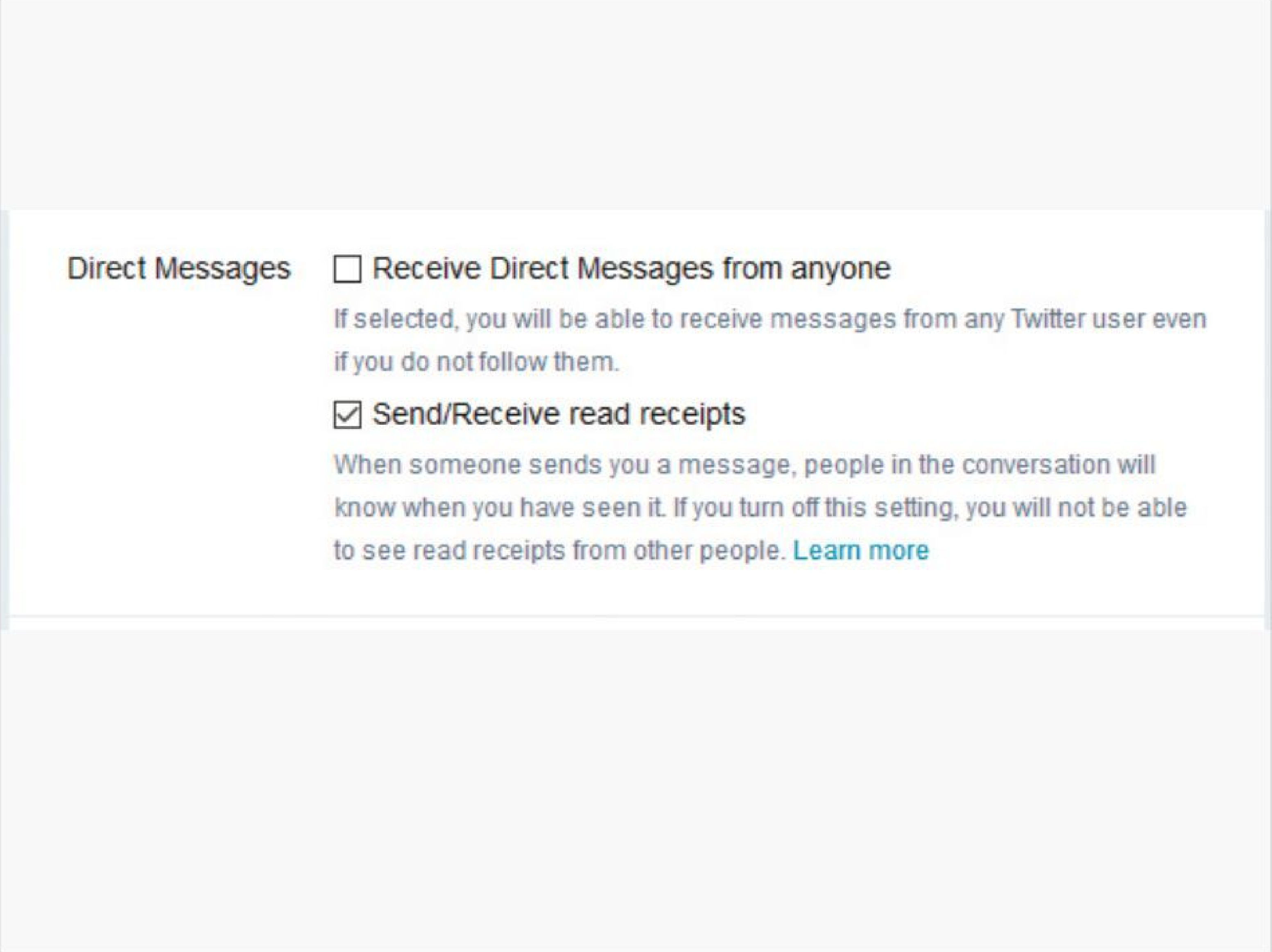
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location ☐ Add a location to my Tweets

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Further down the Privacy and safety section, make sure that the Direct Messages option, Receive Direct Messages From Anyone is unticked. This way you won't get messages from anyone on Twitter, just those who you follow.



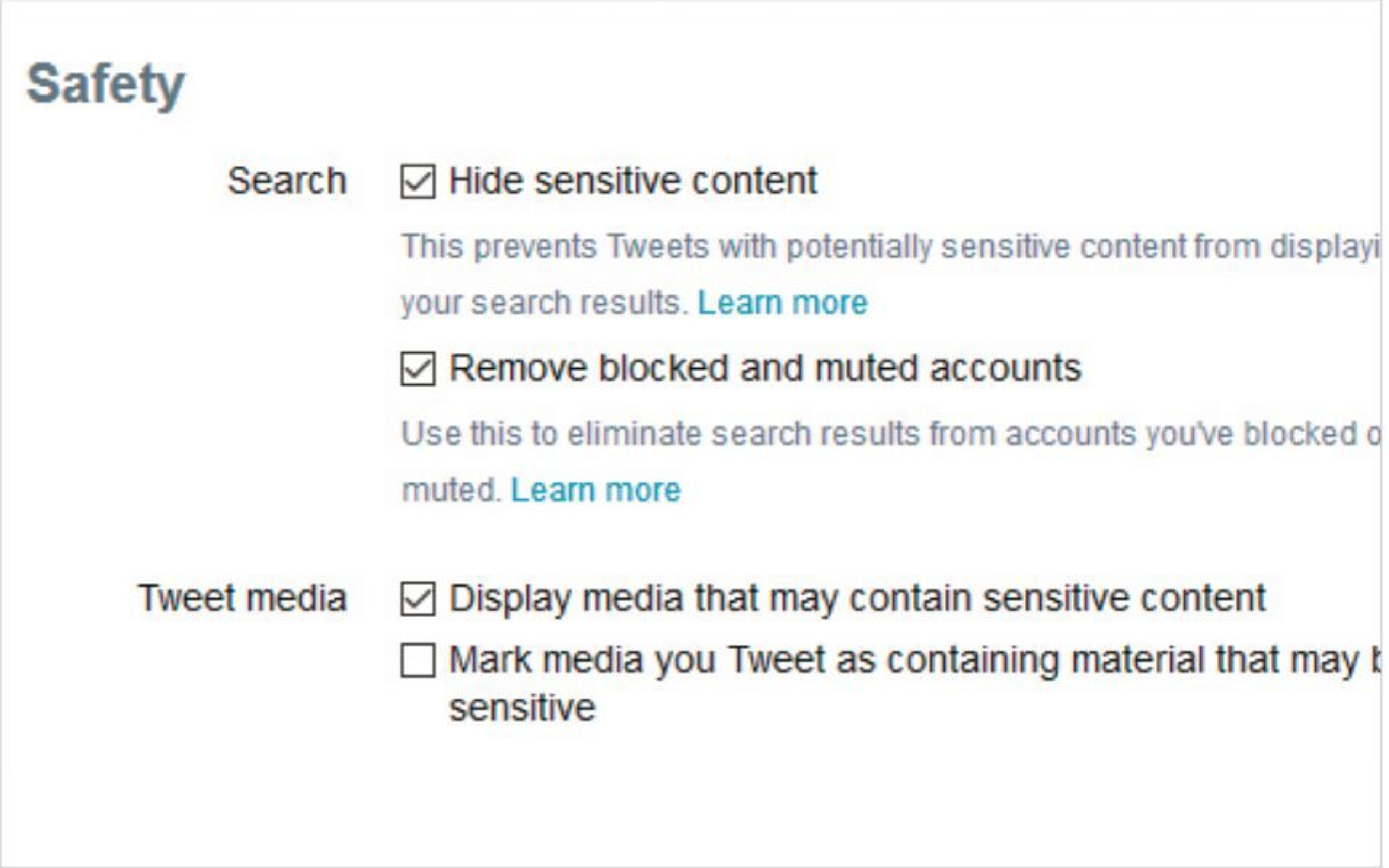
Direct Messages ☐ Receive Direct Messages from anyone

If selected, you will be able to receive messages from any Twitter user even if you do not follow them.

☑ Send/Receive read receipts

When someone sends you a message, people in the conversation will know when you have seen it. If you turn off this setting, you will not be able to see read receipts from other people. Learn more

Just under the Direct Messages options, look to the Safety section. Here you can opt whether to hide Tweets that may contain sensitive content, remove blocked or muted accounts or display media that may also contain sensitive content.



Safety

Search ☑ Hide sensitive content

This prevents Tweets with potentially sensitive content from displayi your search results. Learn more

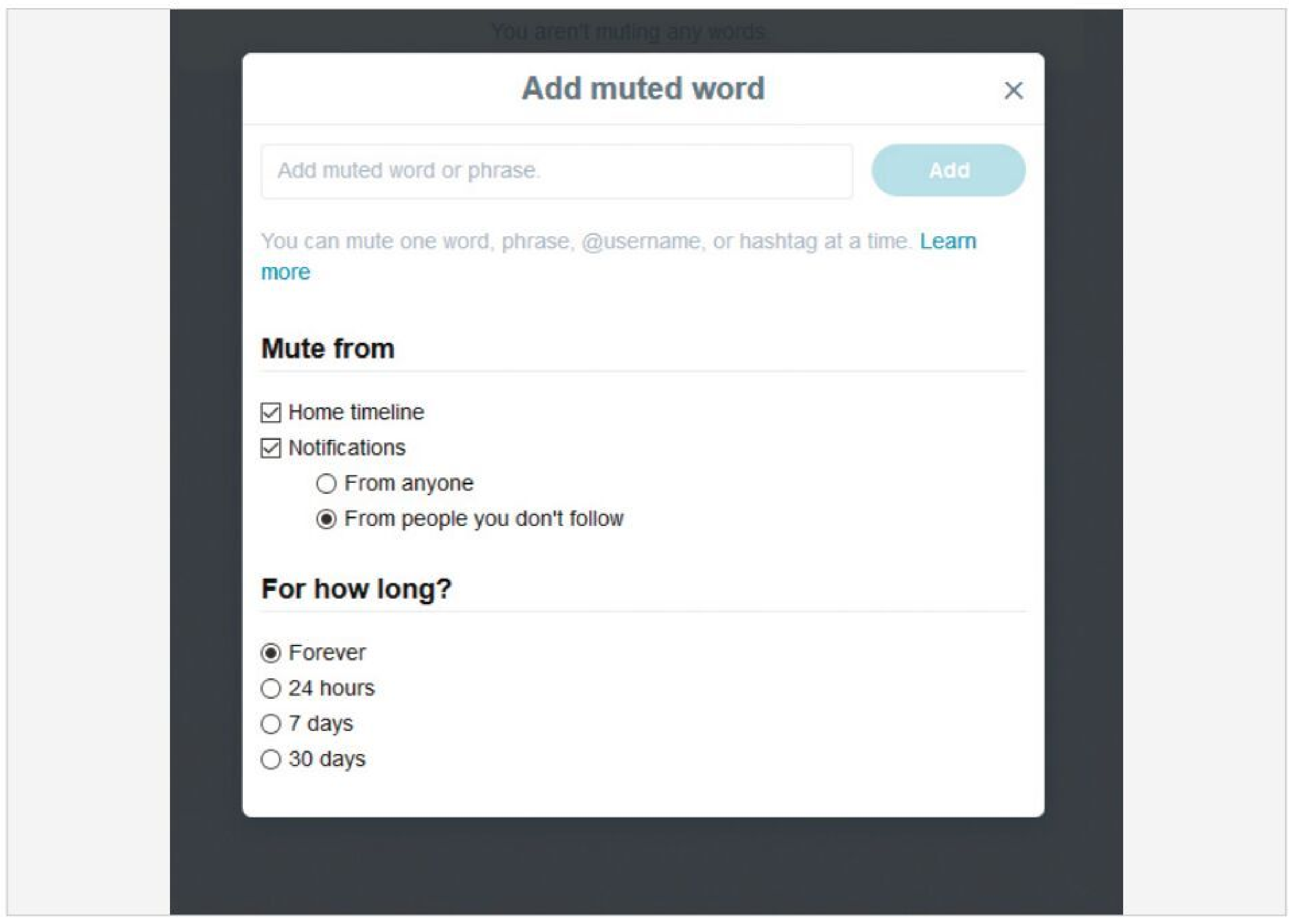
☑ Remove blocked and muted accounts

Use this to eliminate search results from accounts you've blocked o muted. Learn more

Tweet media ☑ Display media that may contain sensitive content

☐ Mark media you Tweet as containing material that may b sensitive

To the left-hand options pane, click on the Muted Words section. With this option you're able to hide certain words, phrases, usernames or hash tags. This is a great option to mass block any content you never want to see, or that contains inappropriate content.



You aren't muting any words.

Add muted word

You can mute one word, phrase, @username, or hashtag at a time. Learn more

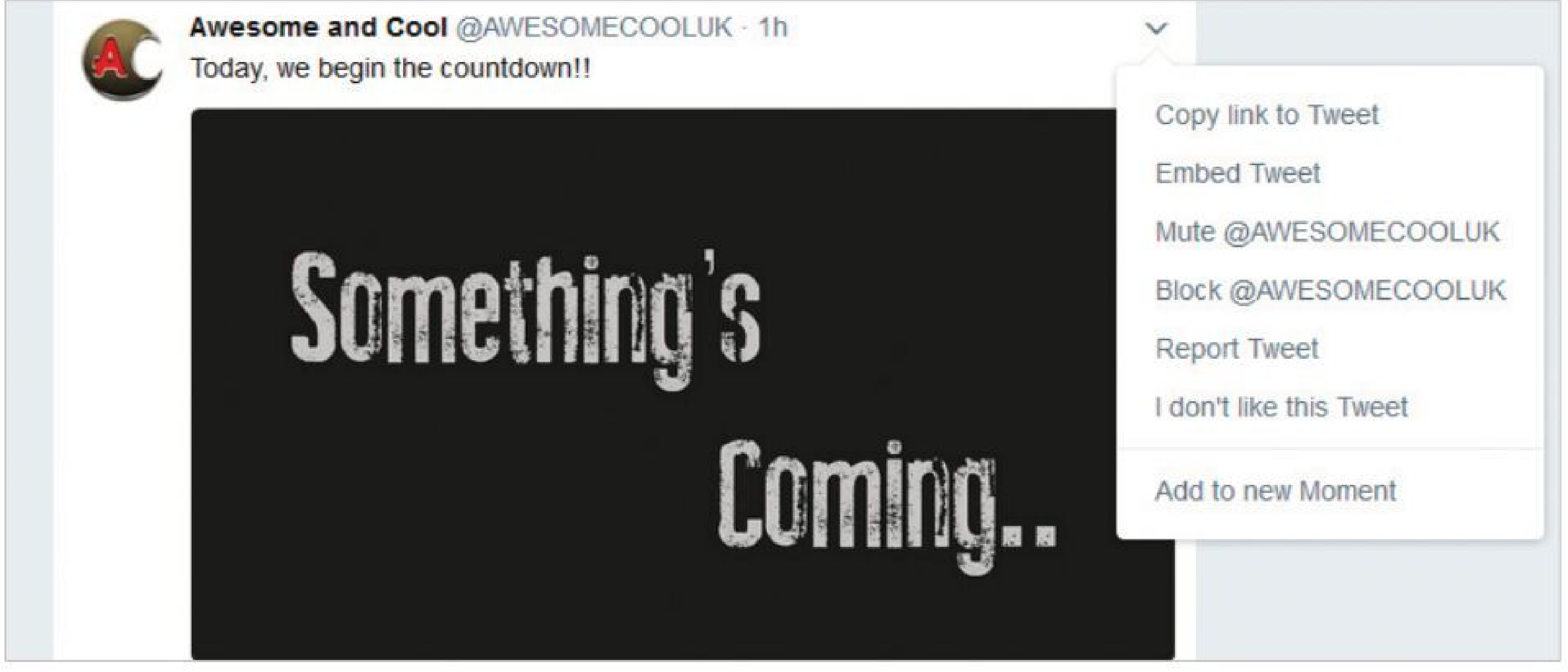
Mute from

☑ Home timeline
☑ Notifications
  ○ From anyone
  ● From people you don't follow

For how long?

● Forever
○ 24 hours
○ 7 days
○ 30 days

If you see a Tweet from a user you don't like the look of, or is offensive in some way or form, you have several options available to you. Click the down-arrow next to the user's name and you can Mute, Block, Report or simply opt for I Don't Like This Tweet.

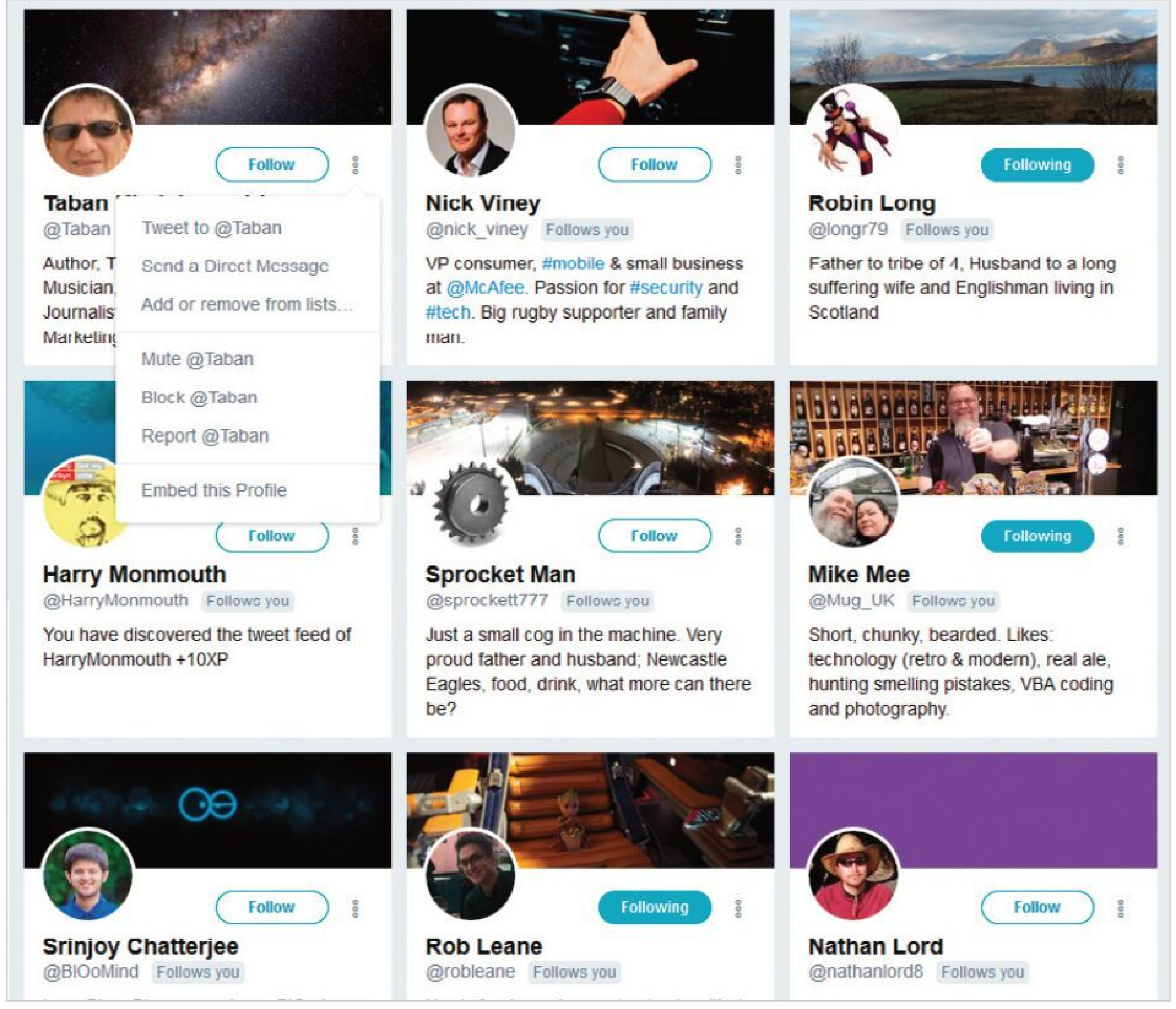


Awesome and Cool @AWESOMECOOLUK · 1h

Today, we begin the countdown!!

Something's
Coming..
Copy link to Tweet
Embed Tweet
Mute @AWESOMECOOLUK
Block @AWESOMECOOLUK
Report Tweet
I don't like this Tweet
Add to new Moment

As a Twitter user who hasn't enabled privacy, you're open to anyone finding and following you. You get an update as soon as someone does follow you and you then have the option to Mute, Block, Report or remove the user. Don't be afraid to remove a user if you don't know or trust them.



Taban
@Taban
Author, T
Musician,
Journalis
Marketing

Nick Viney
@nick_viney Follows you
VP consumer, #mobile & small business at @McAfee. Passion for #security and #tech. Big rugby supporter and family man.

Robin Long
@longr79 Follows you
Father to tribe of 4, Husband to a long suffering wife and Englishman living in Scotland

Harry Monmouth
@HarryMonmouth Follows you
You have discovered the tweet feed of HarryMonmouth +10XP

Sprocket Man
@sprockett777 Follows you
Just a small cog in the machine. Very proud father and husband; Newcastle Eagles, food, drink, what more can there be?

Mike Mee
@Mug_UK Follows you
Short, chunky, bearded. Likes: technology (retro & modern), real ale, hunting smelling pistakes, VBA coding and photography.

Srinjoy Chatterjee
@BlOoMind Follows you

Rob Leane
@robleane Follows you

Nathan Lord
@nathanlord8 Follows you

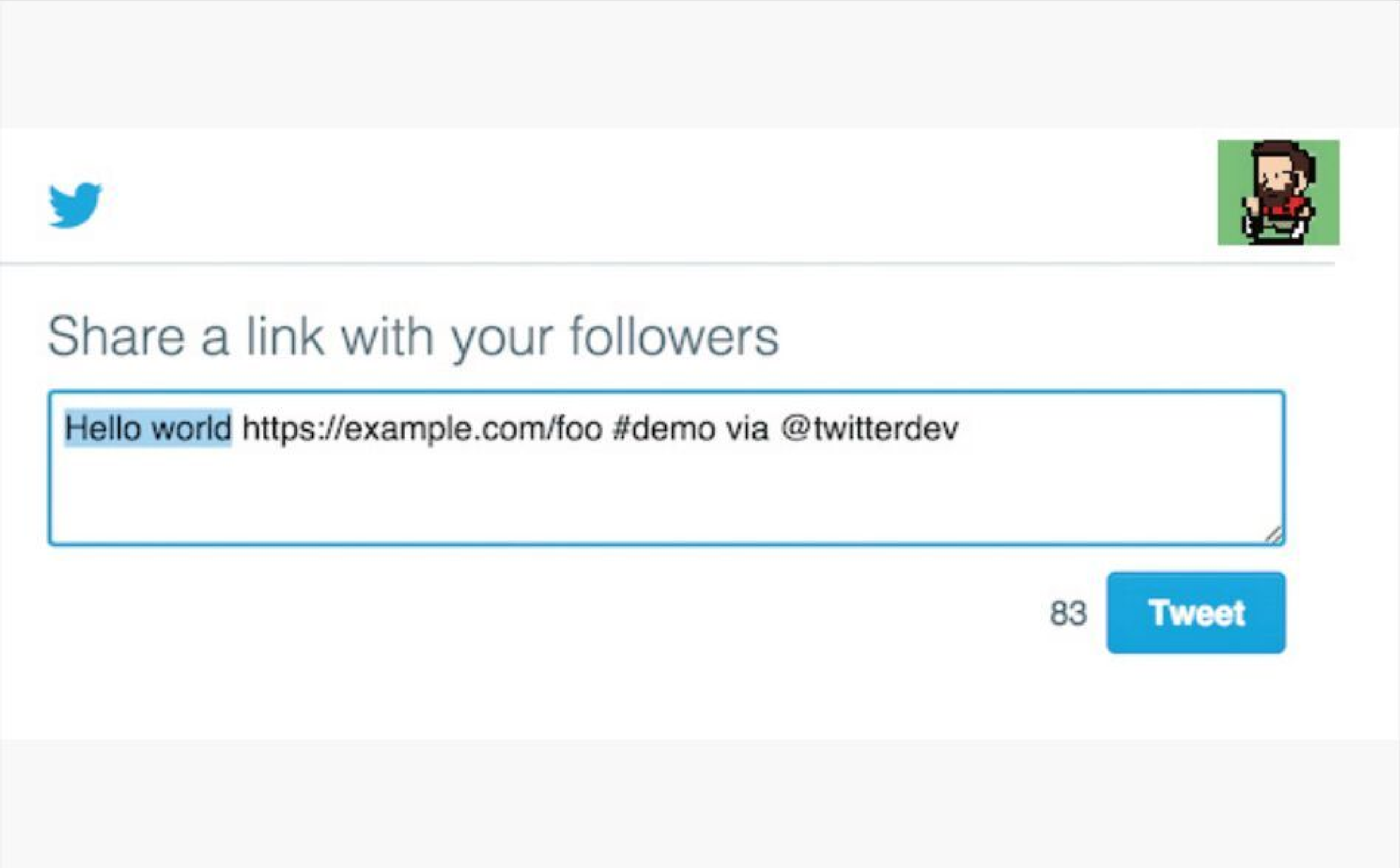
Follow
Following
Tweet to @Taban
Send a Direct Message
Add or remove from lists...
Mute @Taban
Block @Taban
Report @Taban
Embed this Profile

Just as with Facebook posts, don't be fooled into commenting on posts that are phishing attempts. These are created to farm for active accounts and gather information about users' tweets, and any personal details.

Try not to reply to any Direct Messages sent to you on Twitter. Whilst some messages and accounts are real, perhaps a job offer for example, many are simply Twitter bots phishing for active accounts and details.

DIRECT
MESSAGES

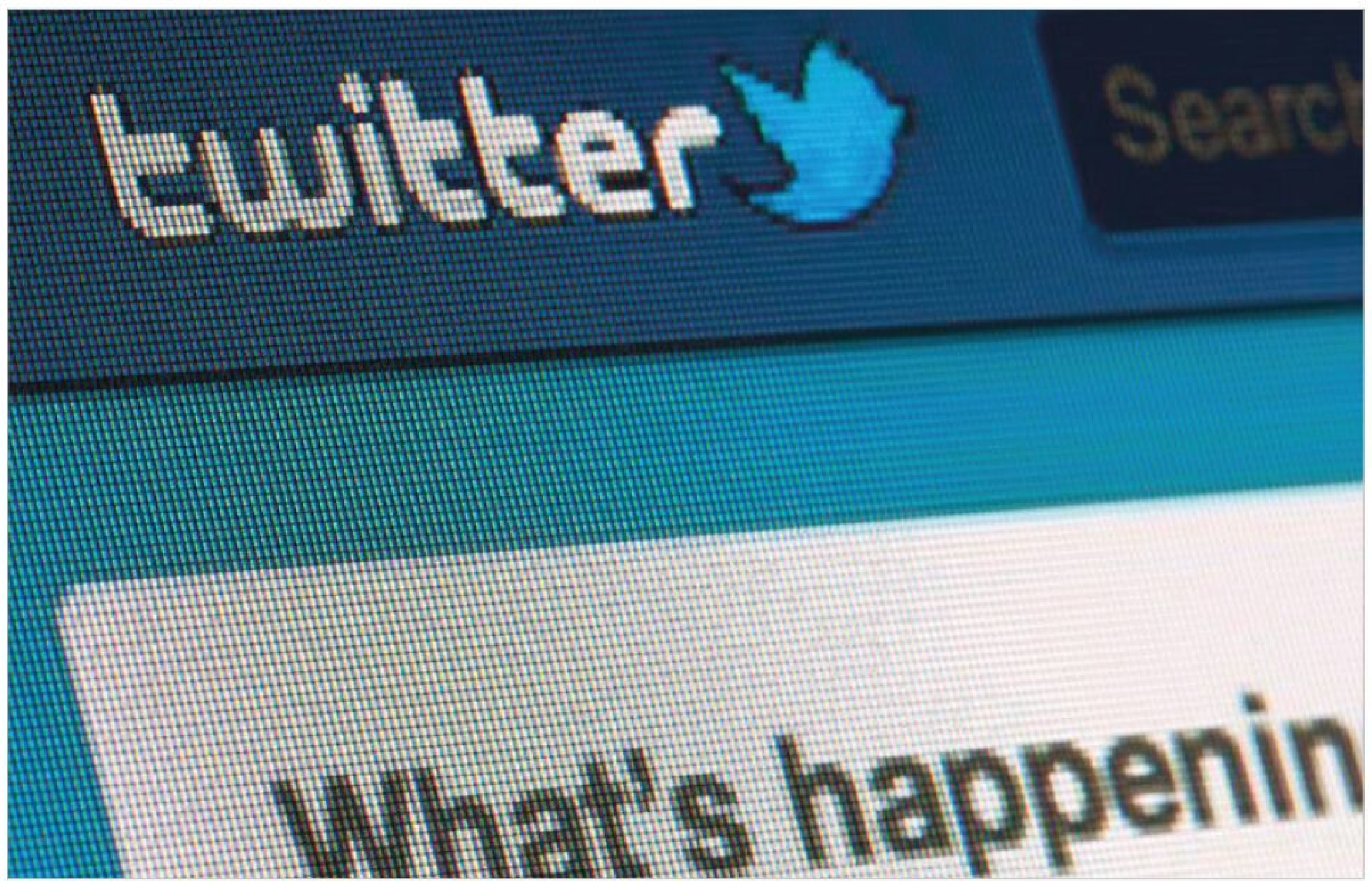
Never click on any links that appear in a Tweet or as part of a Direct Message. Unless you specifically know the user and can trust their Tweets or messages; the link may lead you to a site that's riddled with malware or further scams.



Share a link with your followers

Hello world https://example.com/foo #demo via @twitterdev

Always think before you reply to any Tweets, post your own or upload any images. It's very easy to offend and become involved in a heated war over something you don't want to be a part of. Don't become the victim of anyone baiting you into an argument. If you are, then sign off and leave the group.



twitter
Search
What's happenin

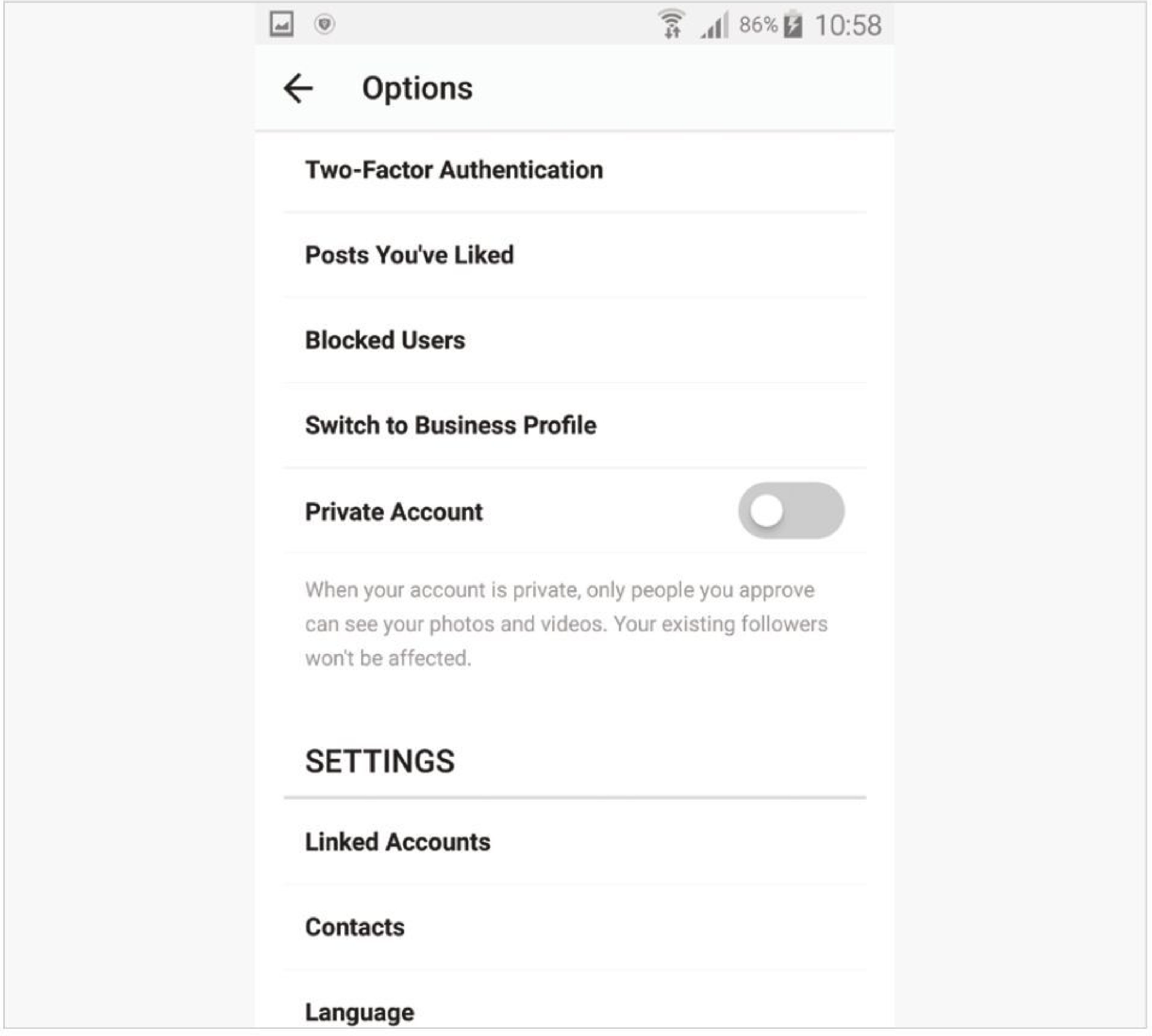
Staying Safe with Instagram for Teens

Much of today’s Internet youth has moved from Facebook and now inhabits Instagram. This social media platform is used by celebrities, politicians and a user base of over 700 million. Needless to say, it’s population is varied and contains those who you wouldn’t want contacting you.

Insta-scam

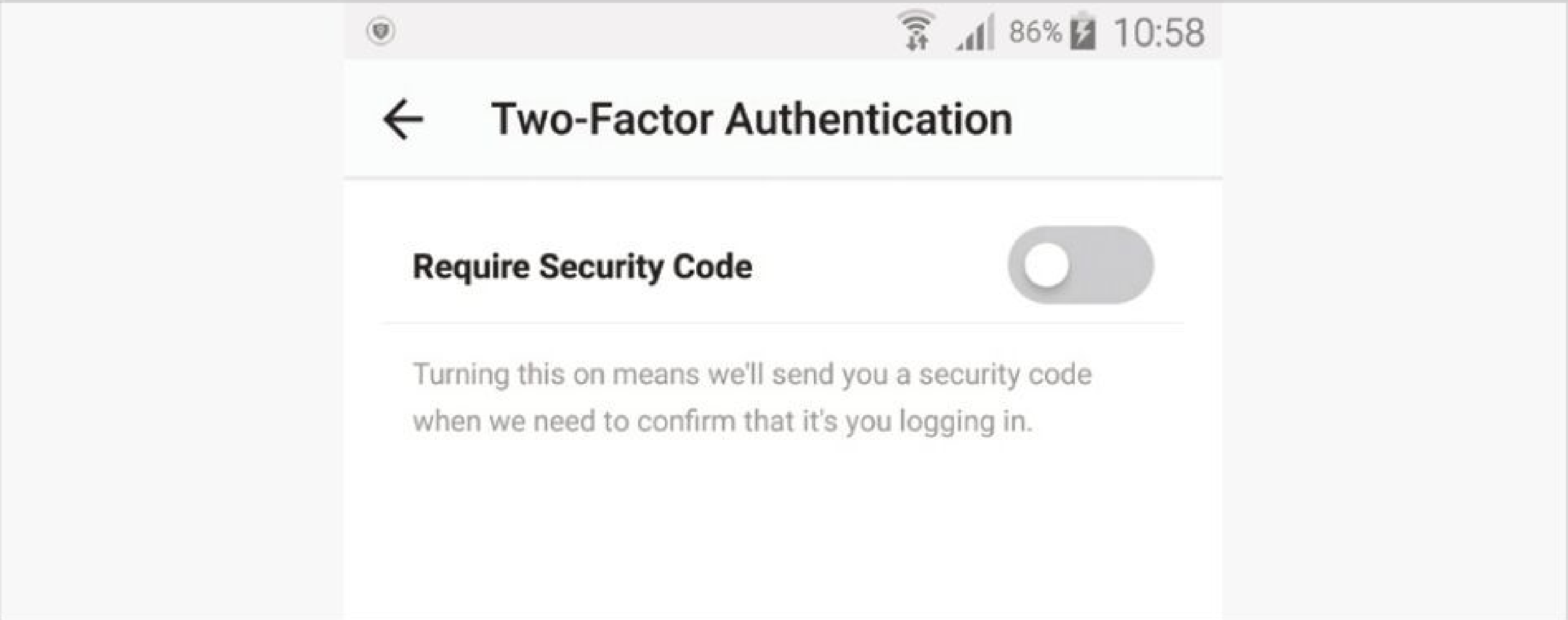
In compliance with the Children’s Online Privacy Protection Act, Instagram requires that its users’ minimum age to sign up is 13 but even as a young teen, there’s still plenty to do to help improve your safety.

Instagram is a simple photo and sharing app but there’s plenty of material and content out there that shouldn’t be viewed by minors. That being the case, tap the person (profile) icon in the bottom right, then the three vertical dots in the top right. This opens the Instagram Options window. From there, scroll down and enable Private Account.


86% 10:58
Options
Two-Factor Authentication
Posts You've Liked
Blocked Users
Switch to Business Profile
Private Account
SETTINGS
Linked Accounts
Contacts
Language

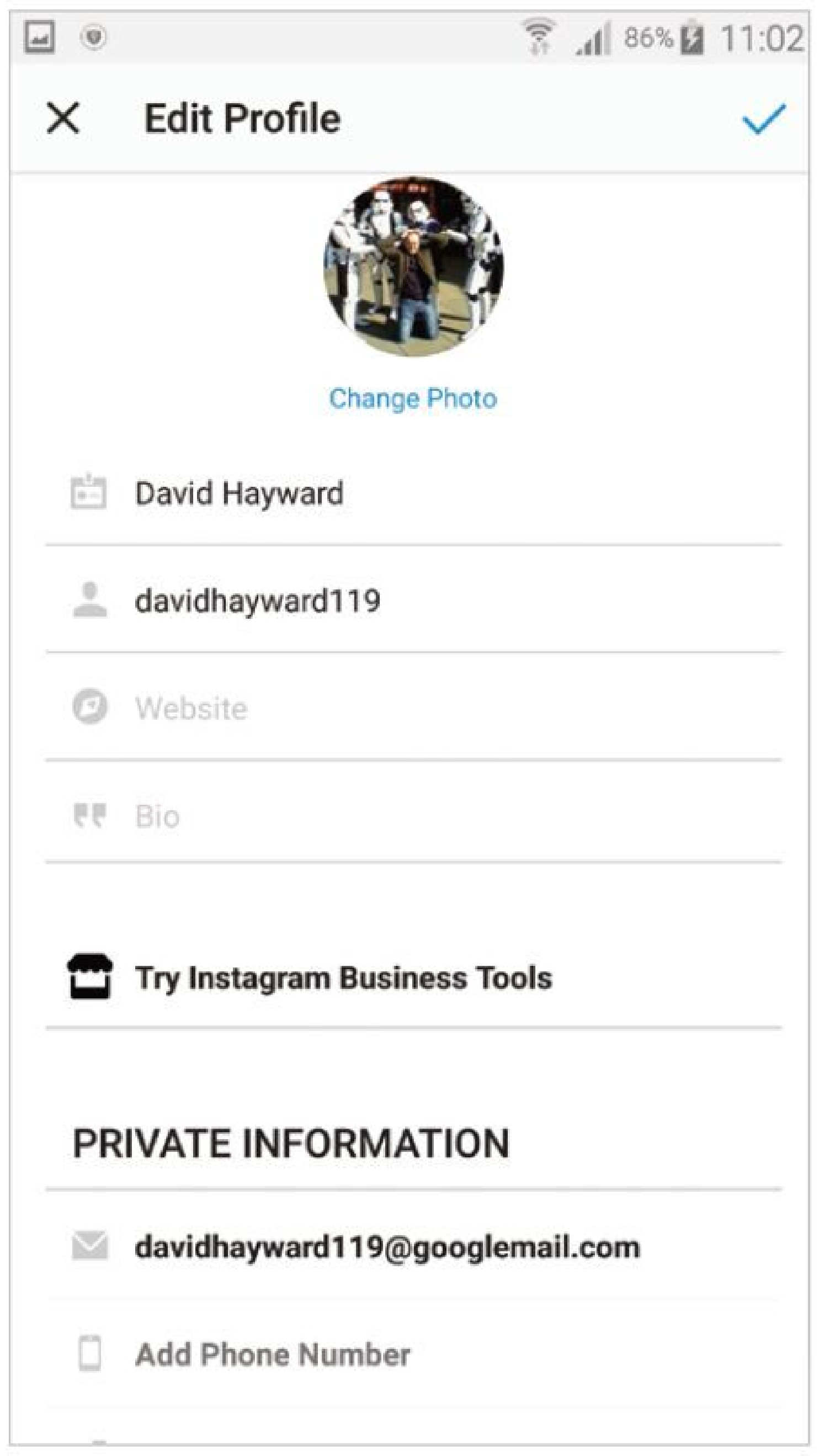
When your account is private, only people you approve can see your photos and videos. Your existing followers won't be affected.

Private Accounts are visible, but not the content you’ve posted. Anyone who wants to follow you will need to send a request, so you can easily decline any users. Whilst still in the Account section, scroll up and consider enabling Two-Factor Authentication, for additional security.


86% 10:58
Two-Factor Authentication
Require Security Code

Turning this on means we'll send you a security code when we need to confirm that it's you logging in.

Staying in the Account section, tap on Edit Profile. This is where you can create a profile picture and include other information about yourself. It’s up to you how much info you want to add but it’s often best to take a secure-minded approach and not give away too much.

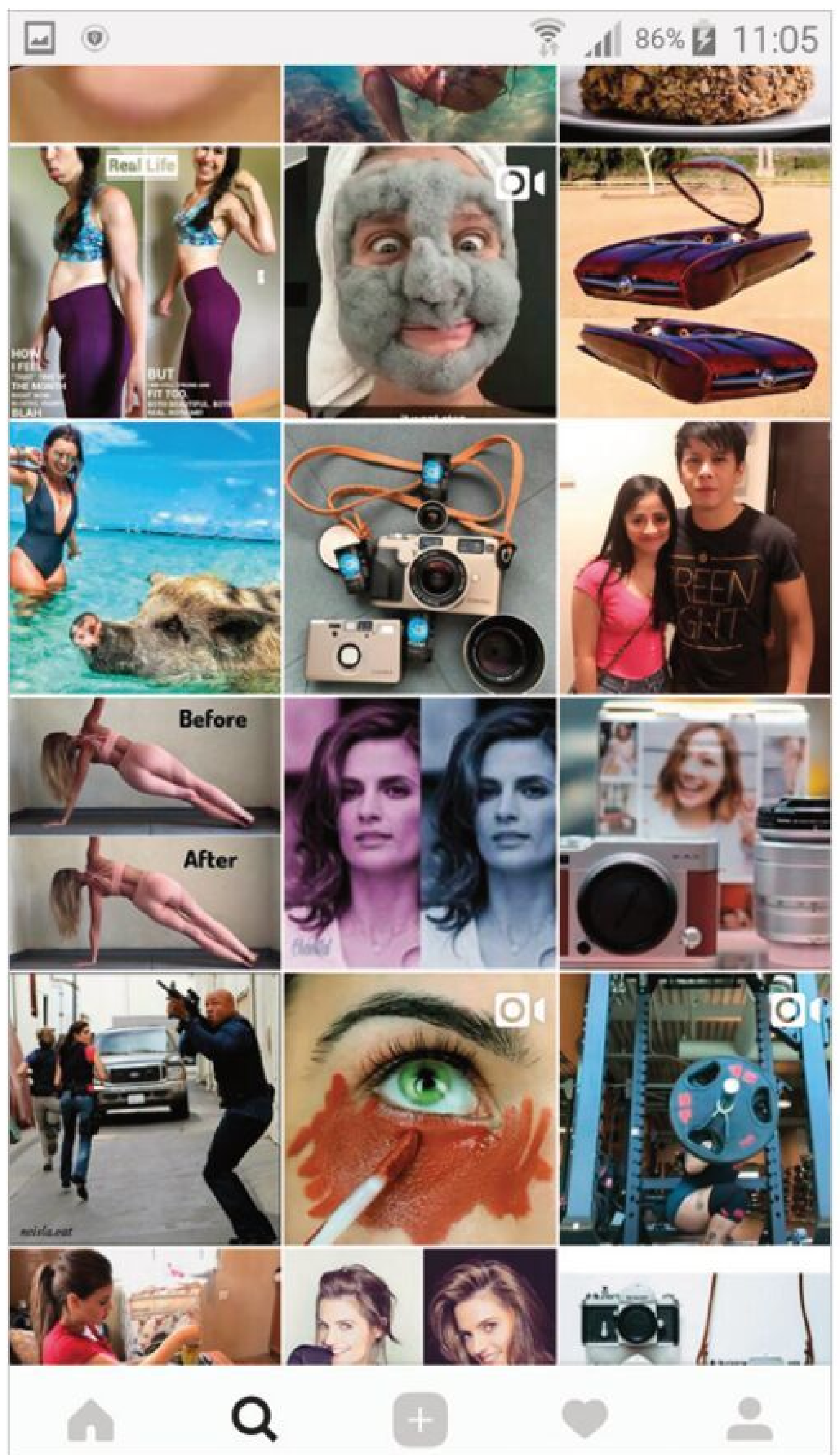

86% 11:02
Edit Profile
Change Photo
Website
Bio
Try Instagram Business Tools
PRIVATE INFORMATION
Add Phone Number

David Hayward

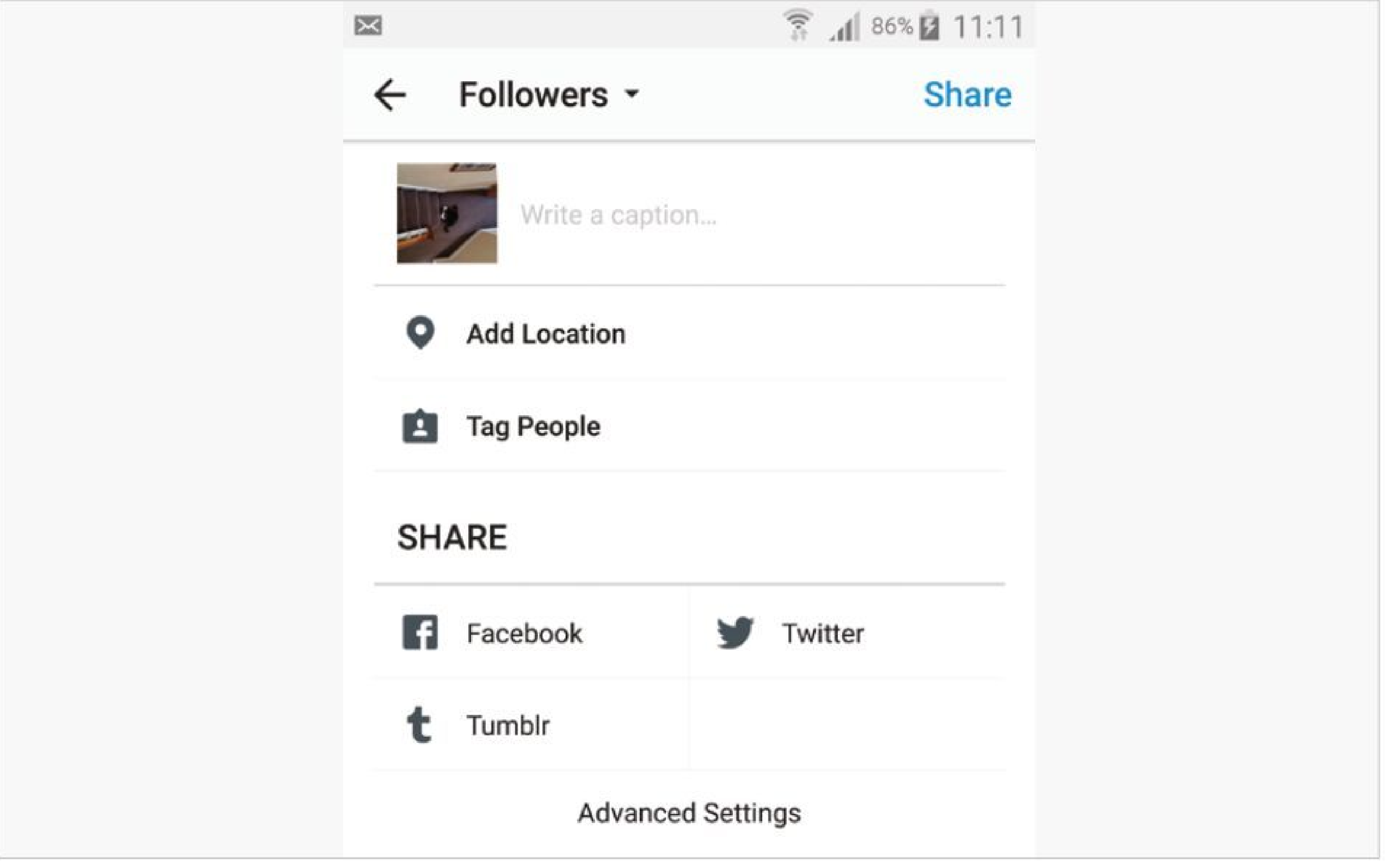
davidhayward119

davidhayward119@googlemail.com

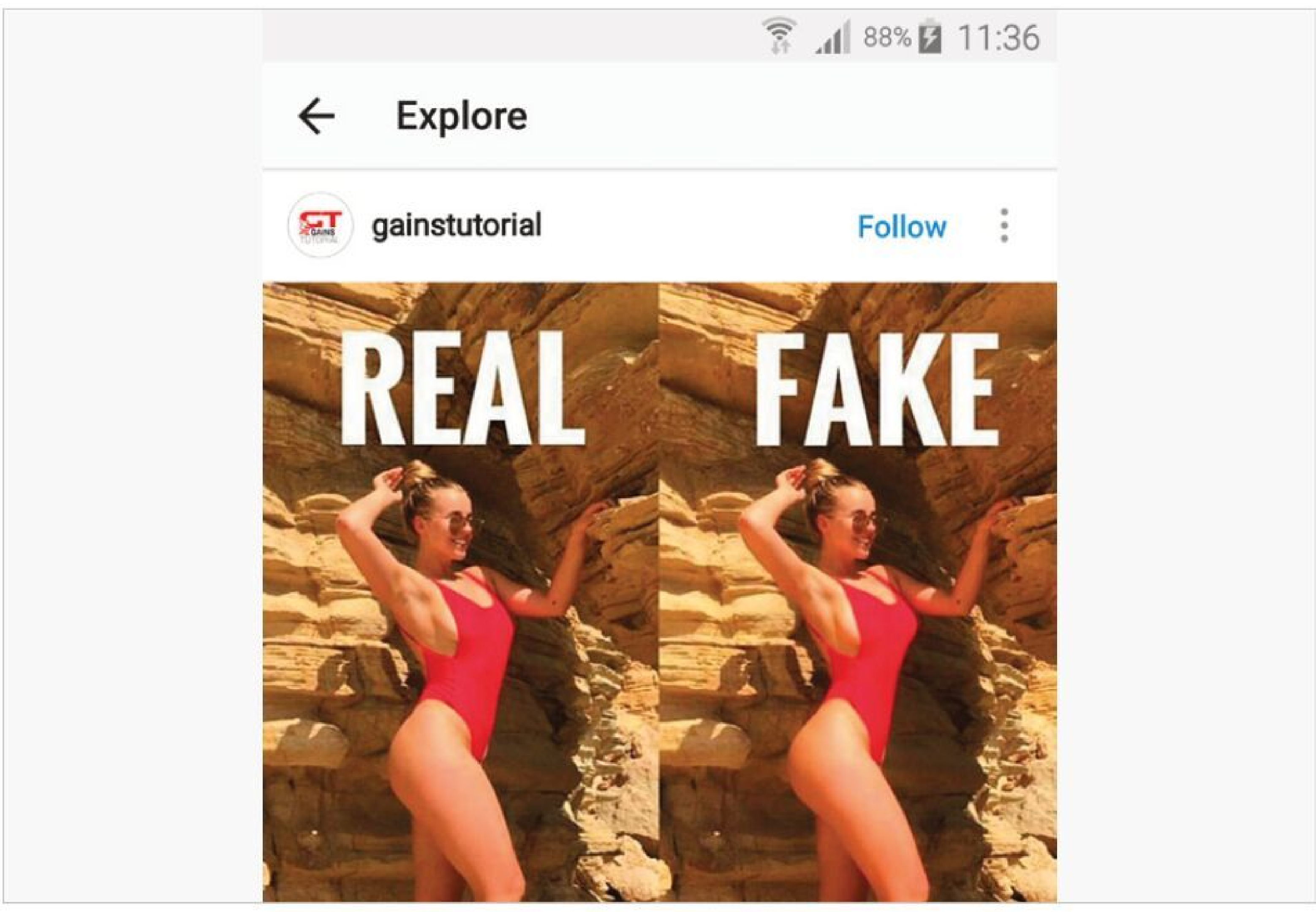
The magnifying glass icon is the Instagram search function. It often displays images and videos based on your likes and who you follow, such as amazing landscapes but it’s also known to insert content that isn’t always appropriate for younger viewers. Don’t open the image, even to report it, it’s best to just ignore it.


86% 11:05
Real Life
Before
After

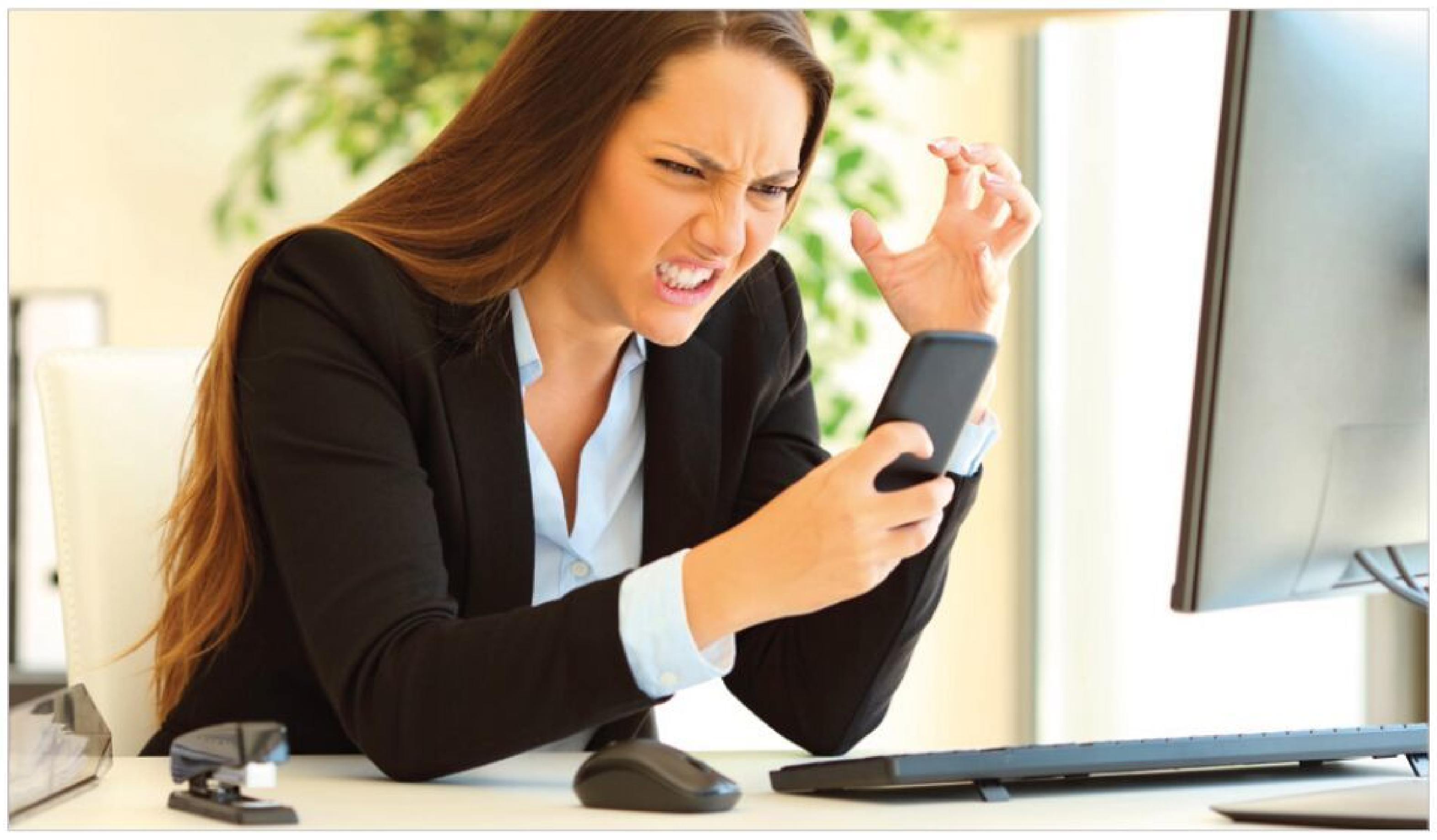
Uploading an image provides multiple options, from choosing a filter, image style and so on, to tagging other people, sharing with other social media platforms and adding a location. It may seem harmless enough but consider not sharing your location, as it's instantly available on Instagram. It doesn't take a genius to locate where you are.



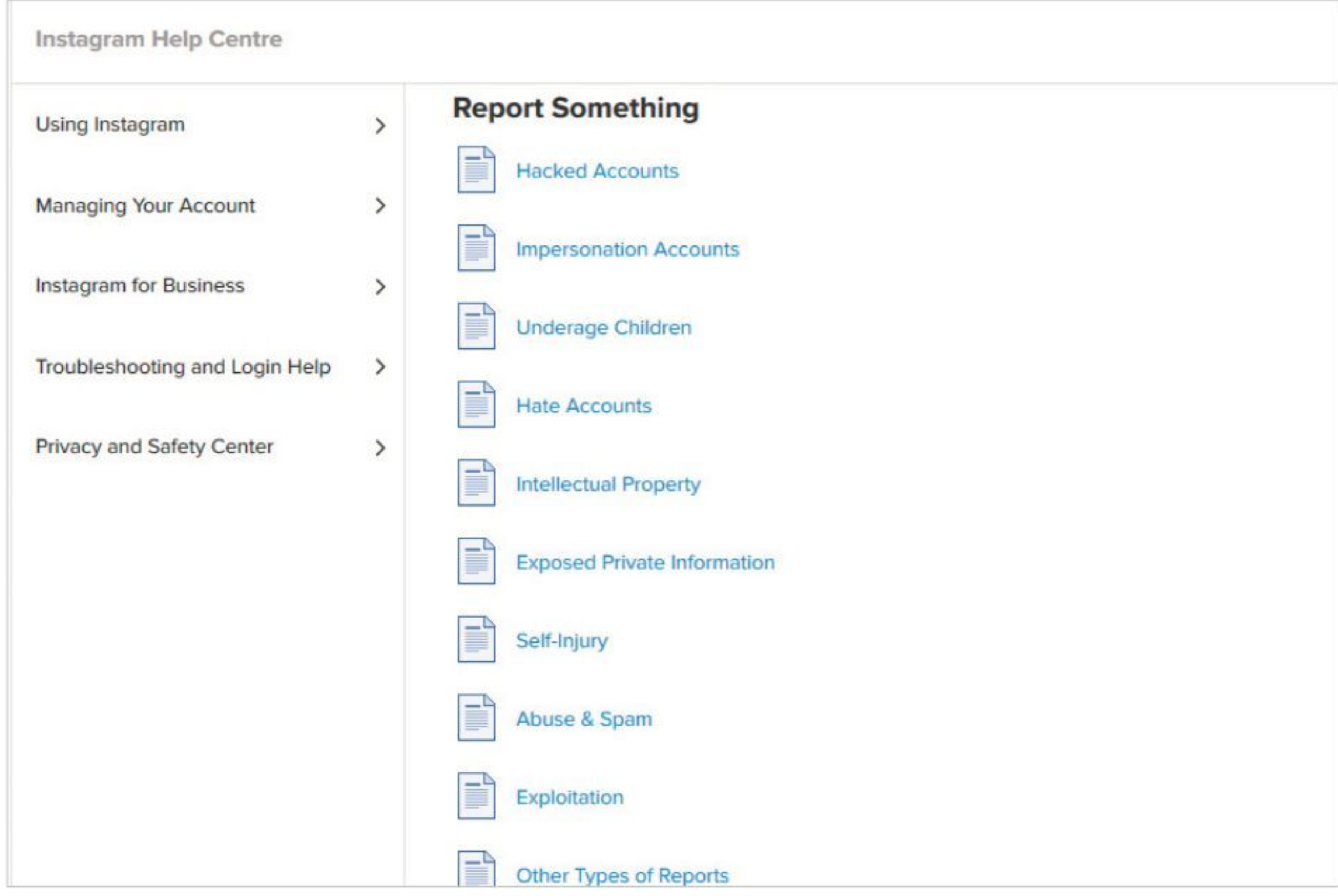
Be wary of what you see on Instagram. This applies to other social media platforms too but Instagram users appear to revel in posting fake or photoshopped images of themselves or others, or even events. It's a huge source of image-aware and body-conscious behaviour, that's influential to younger minds. In short, don't always believe what you see on Instagram.



If you've approved a user, whilst in privacy mode, and they start to send you inappropriate images, video or comments, then make sure that you show a parent or guardian. Don't respond to the sender and don't unfollow or block them until you've shown someone or taken a screenshot of the content.



The Instagram Help Centre is where you can report a user for inappropriate content, abuse, spam, hacked accounts or exposure of private information. It's available from any browser, as well as from the app itself. Be familiar with it, as you may need it someday.



Instagram Help Centre

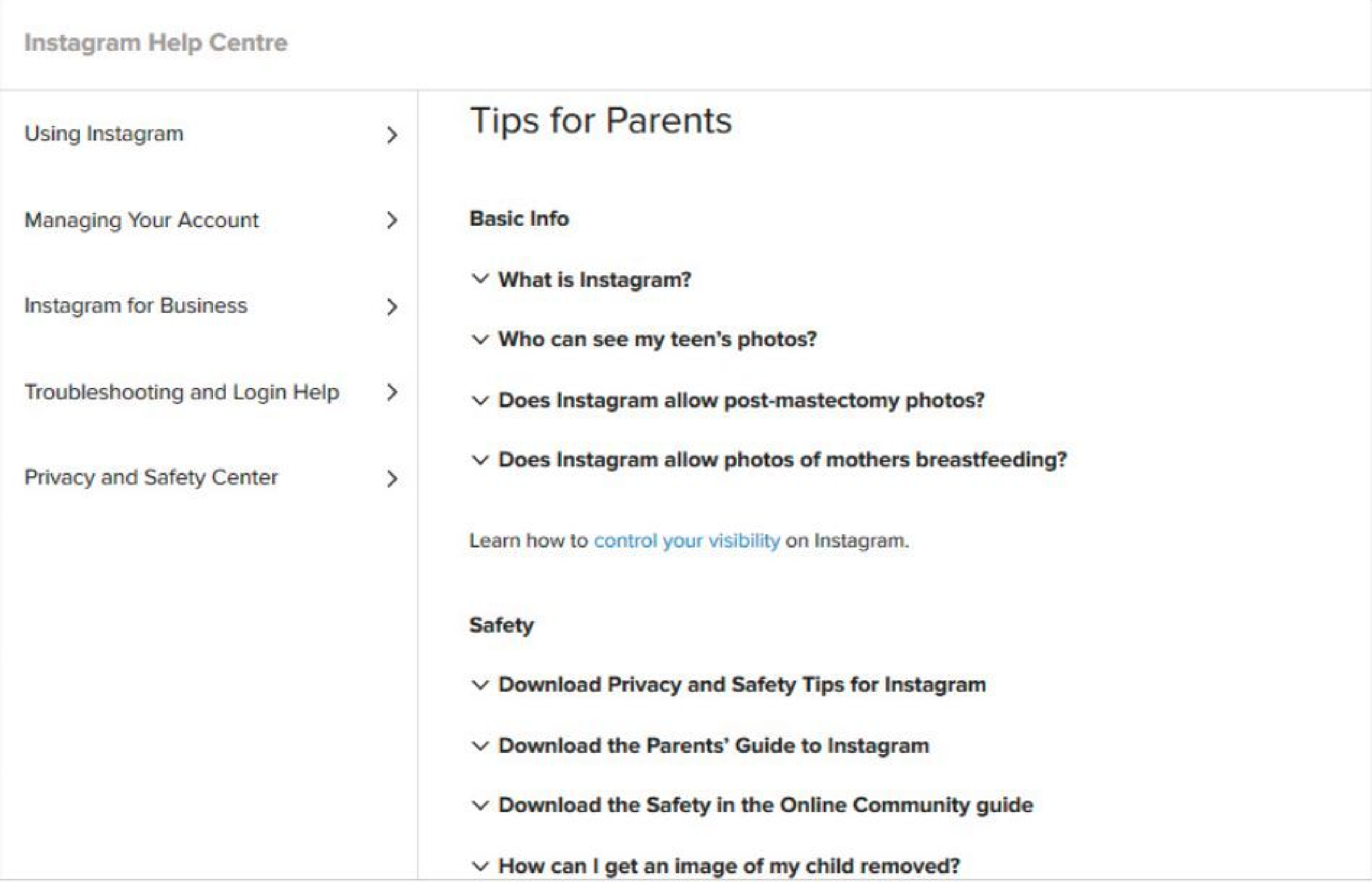
- Using Instagram
- Managing Your Account
- Instagram for Business
- Troubleshooting and Login Help
- Privacy and Safety Center

Report Something

- Hacked Accounts
- Impersonation Accounts
- Underage Children
- Hate Accounts
- Intellectual Property
- Exposed Private Information
- Self-Injury
- Abuse & Spam
- Exploitation
- Other Types of Reports

If you find yourself involved with someone or a group of people who are obviously trying to create some form of hate messaging, bullying or similar, make sure you take any screenshots as proof (in case someone reports the incident) and walk away from the conversation. Block accounts if necessary, to stop further instances happening.

Parents: before you allow your young teen access to Instagram, it's best you have a read through the company's Tips for Parents section. This can be found at **https://help.instagram**.com/154475974694511/?helpref=hc_fnav and includes everything you need to know about what it is and how it works.



Instagram Help Centre

- Using Instagram
- Managing Your Account
- Instagram for Business
- Troubleshooting and Login Help
- Privacy and Safety Center

Tips for Parents

Basic Info

- **What is Instagram?**
- **Who can see my teen's photos?**
- **Does Instagram allow post-mastectomy photos?**
- **Does Instagram allow photos of mothers breastfeeding?**

Learn how to control your visibility on Instagram.

Safety

- **Download Privacy and Safety Tips for Instagram**
- **Download the Parents' Guide to Instagram**
- **Download the Safety in the Online Community guide**
- **How can I get an image of my child removed?**

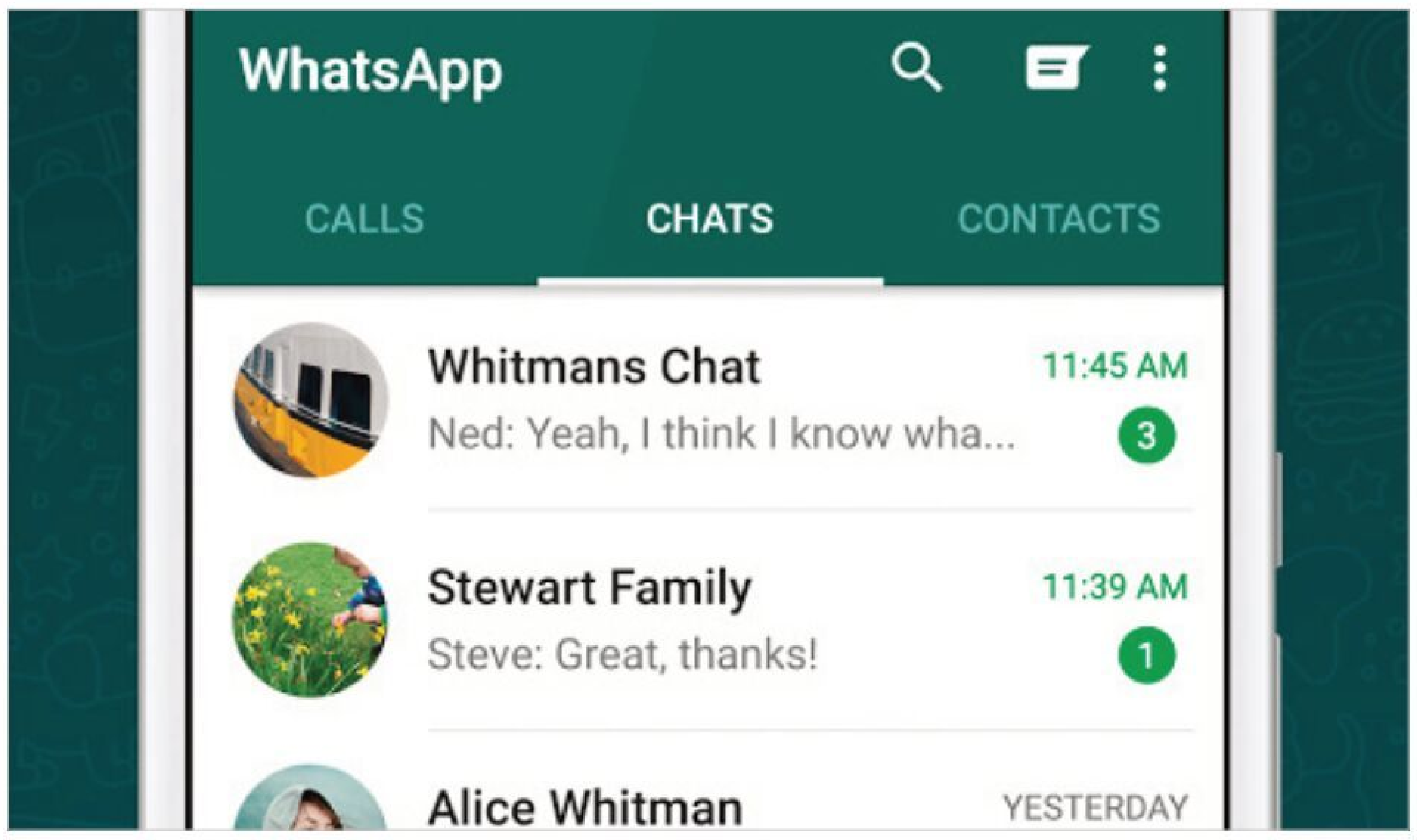
Staying Safe with WhatsApp for Teens

WhatsApp is a free messenger app that can make Internet voice and video calls, send messages, images and other content. It's a little safer than some social media platforms, as you need a user's phone number before being able to add them; but there's always room for further security.

What App?

There's plenty you can do to improve your privacy and security and remain safe when using WhatsApp. Here are ten tips for teens and parents when using this popular app.

According to WhatsApp's terms, the minimum age needed is thirteen years old before a young person is allowed to use the service. Thankfully young teens are only able to contact those who they have added to their WhatsApp account but it's best to occasionally check their contact list in case of someone unknown being added.

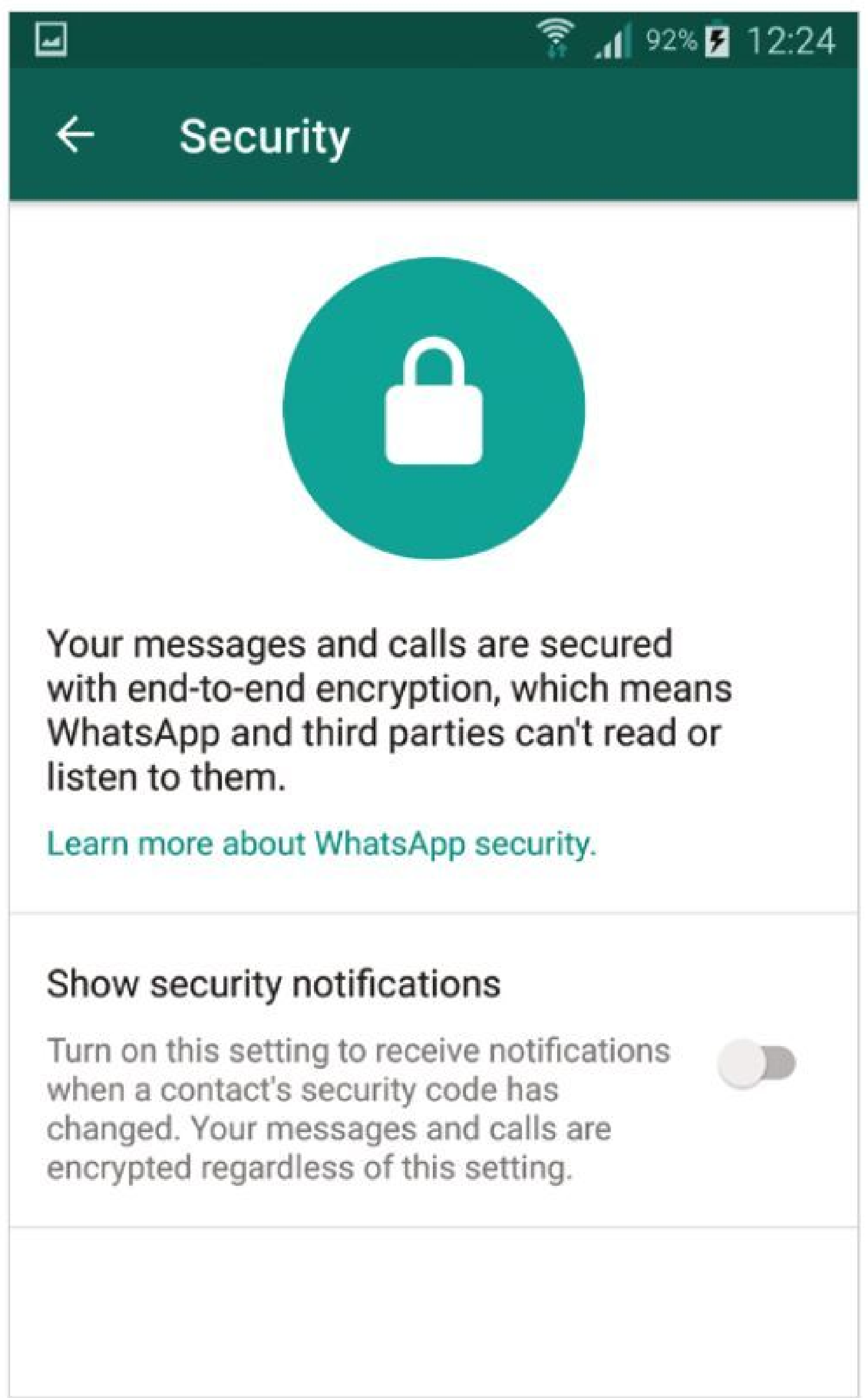


Whitmans Chat 11:45 AM
Ned: Yeah, I think I know wha... 3

Stewart Family 11:39 AM
Steve: Great, thanks! 1

Alice Whitman YESTERDAY

WhatsApp has a high-degree of encryption and security already built-in; however, by tapping the Security option within the Account option, you're able to display any security notifications that may crop up from time to time.



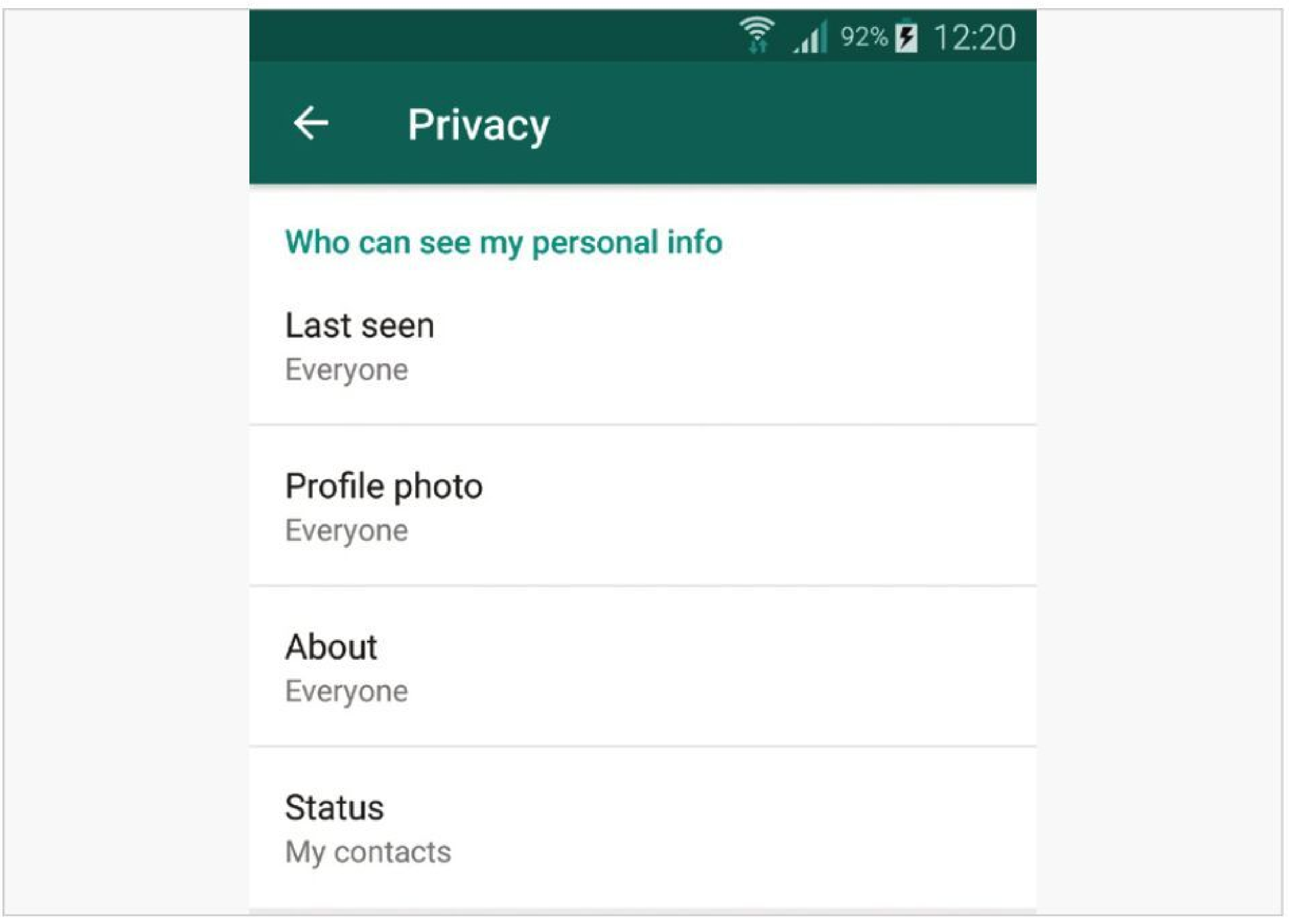
Your messages and calls are secured with end-to-end encryption, which means WhatsApp and third parties can't read or listen to them.

Learn more about WhatsApp security.

Show security notifications

Turn on this setting to receive notifications when a contact's security code has changed. Your messages and calls are encrypted regardless of this setting.

Tap the three vertical dots in the top right of the WhatsApp interface, followed by tapping the Settings option. Now tap the Account option, then Privacy. In here you're able to limit the amount of personal information a contact can view, as well as block any contacts.



Who can see my personal info

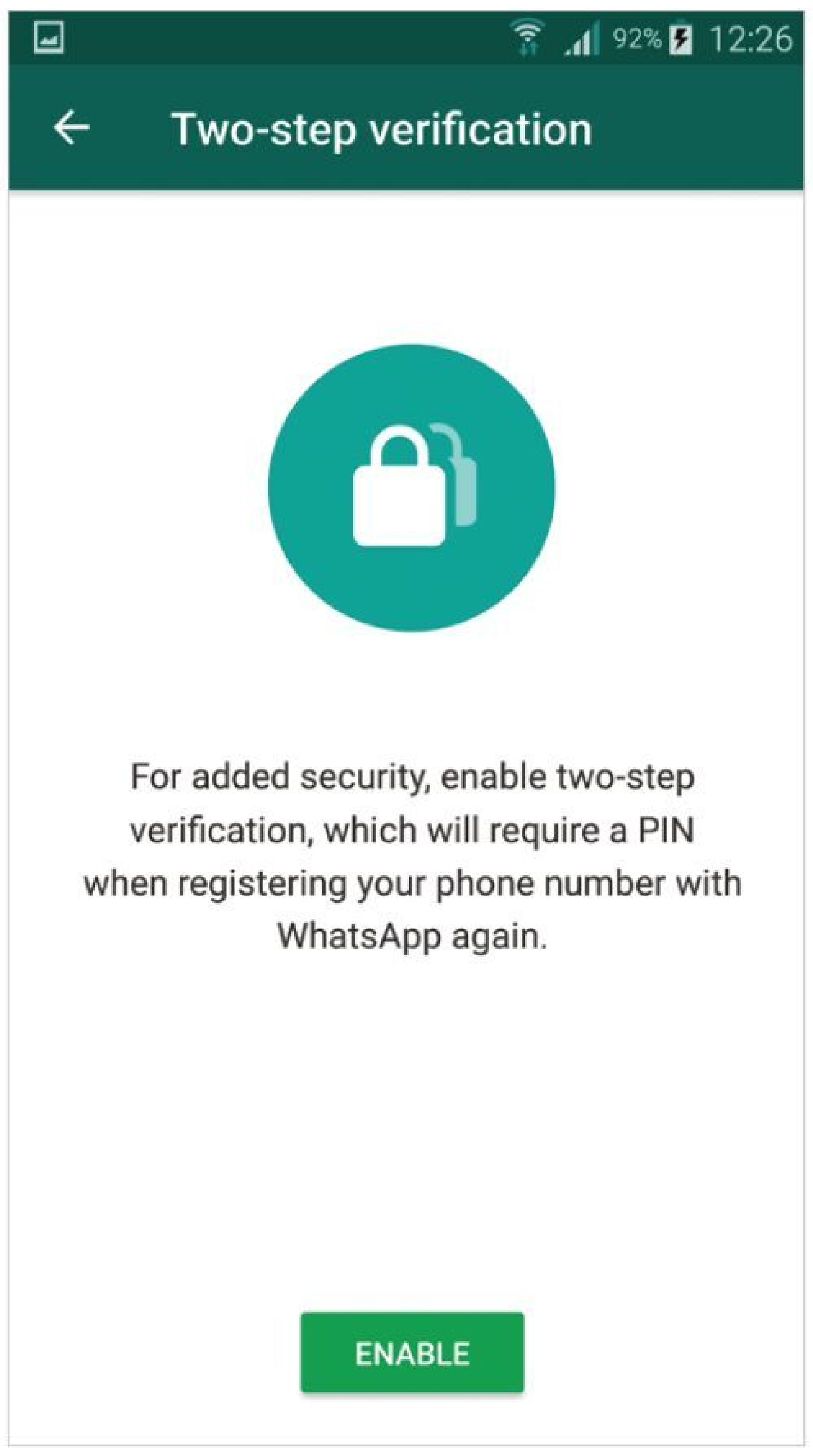
Last seen
Everyone

Profile photo
Everyone

About
Everyone

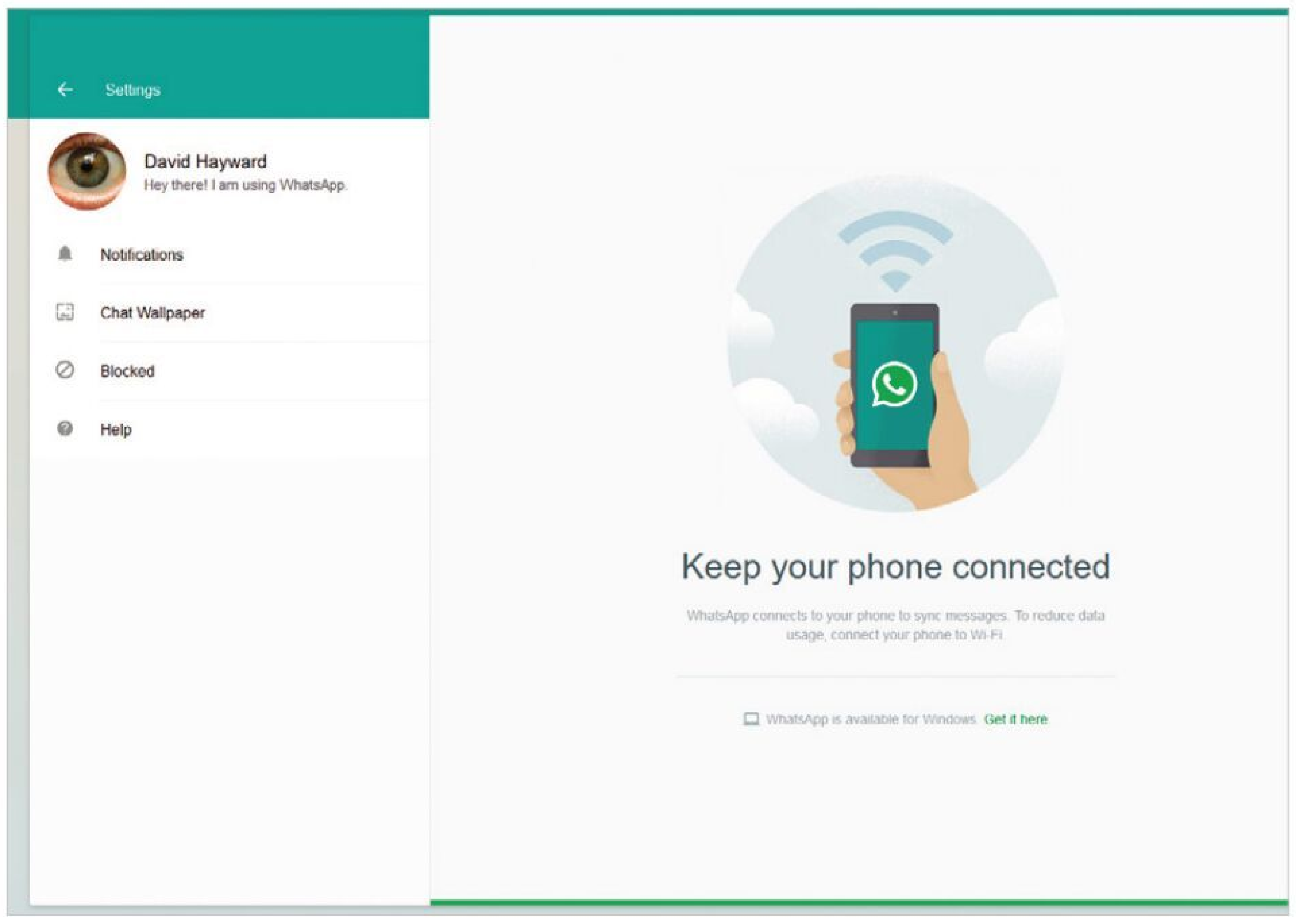
Status
My contacts

Again, from the Account option, tap on the Two-Step Verification setting to set up a PIN in addition to your usual login information. This will enhance the security of your WhatsApp account, should you ever lose your device.



For added security, enable two-step verification, which will require a PIN when registering your phone number with WhatsApp again.

If you're using the web version of WhatsApp, click on the three vertical dots, followed by Settings. Although not as comprehensive as the app's settings, you can set up your notifications and block any users if necessary.

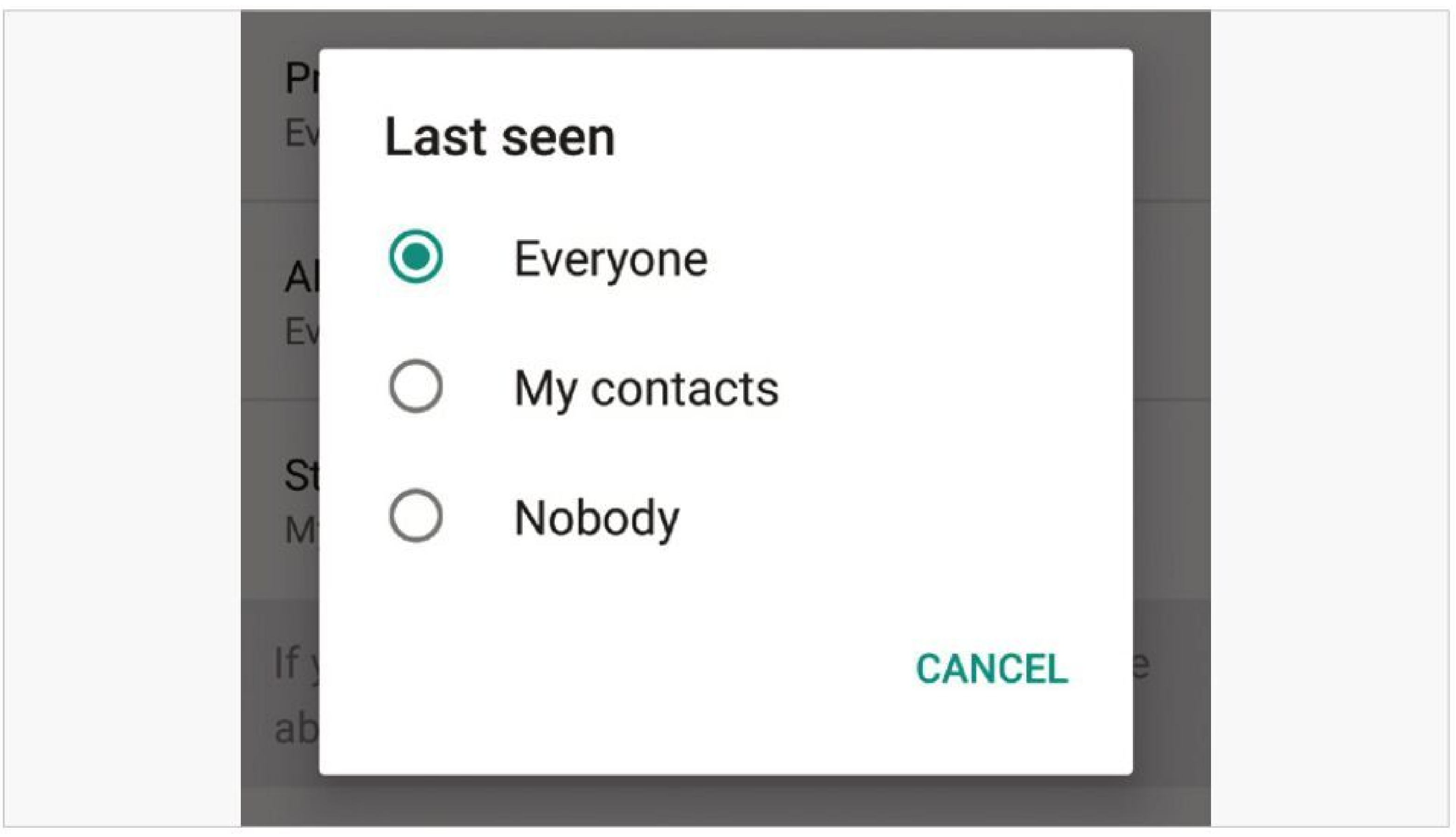

Settings
David Hayward
Hey there! I am using WhatsApp.
Notifications
Chat Wallpaper
Blocked
Help

Keep your phone connected

WhatsApp connects to your phone to sync messages. To reduce data usage, connect your phone to Wi-Fi.

WhatsApp is available for Windows. Get it here

Back to the Privacy settings in the app's Account option, don't forget to limit the Last Seen setting. The three options available are: Everyone, My Contacts and Nobody. This will prevent contacts from seeing where you were when you posted any content.



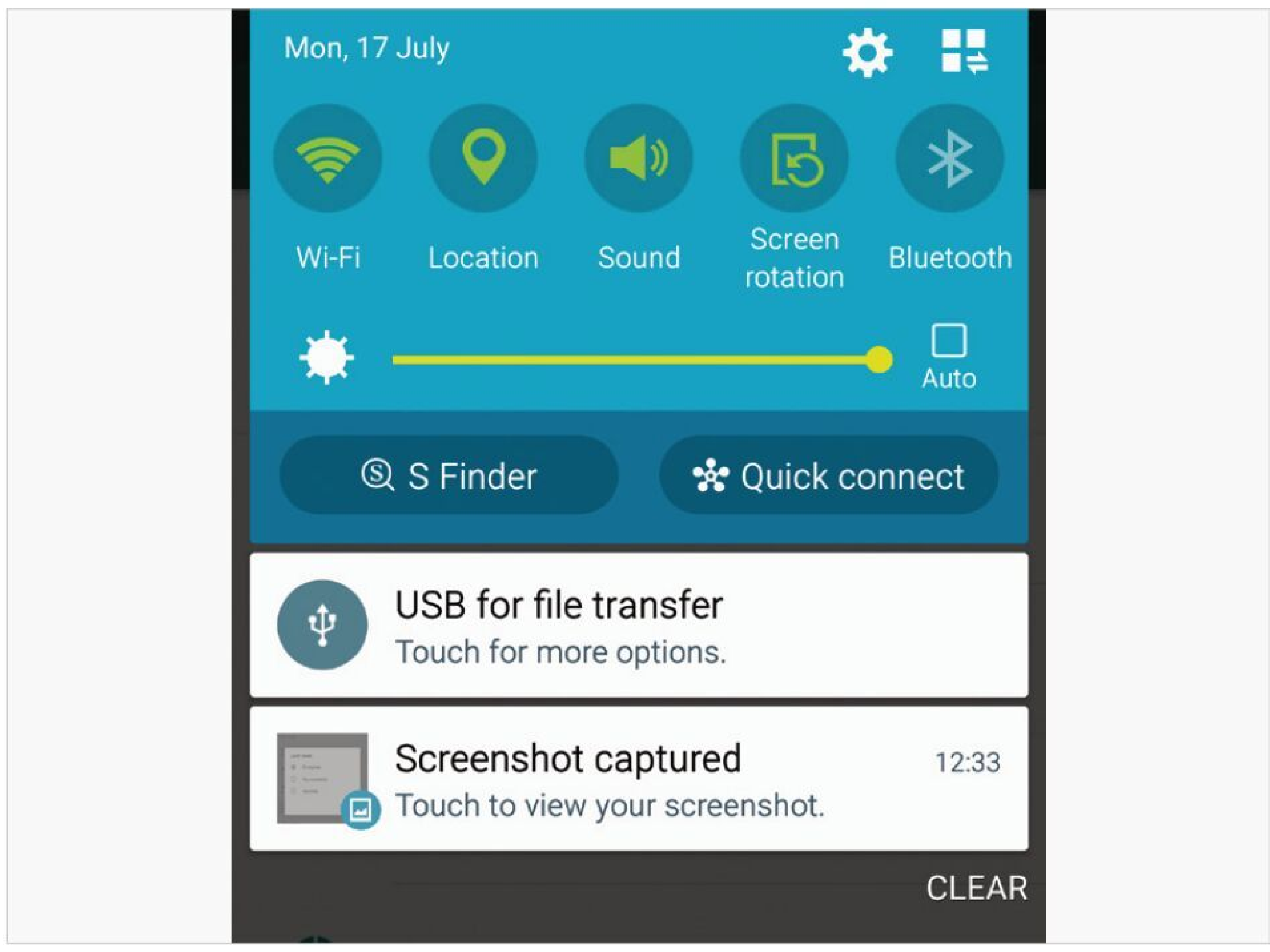
Last seen

● Everyone

○ My contacts

○ Nobody

WhatsApp also utilises the device's built-in Location feature. This enables geo-tagging of content as it's uploaded. If you want to upload something but want to make sure that nobody knows where you are, quickly tap the Location function on your device to disable it before uploading.


Mon, 17 July
Wi-Fi
Location
Sound
Screen rotation
Bluetooth
Auto
S Finder
Quick connect
CLEAR

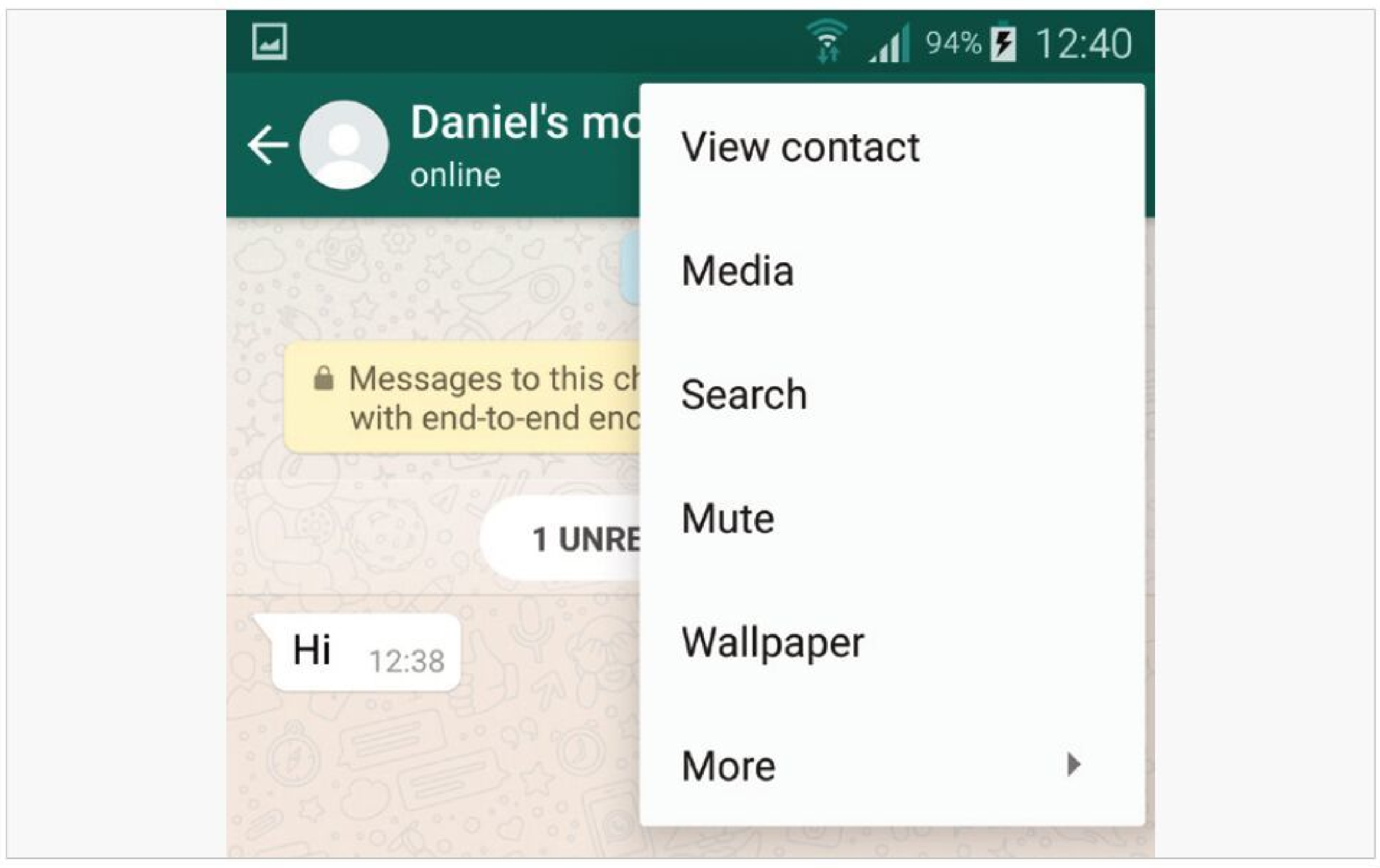
USB for file transfer
Touch for more options.

Screenshot captured 12:33
Touch to view your screenshot.

If someone becomes aggressive or starts to bully you in WhatsApp, take a screenshot and record the evidence, then approach a parent and guardian and show them what's going on. Don't respond to the person and don't block them immediately. Always talk to a parent or guardian before doing anything.

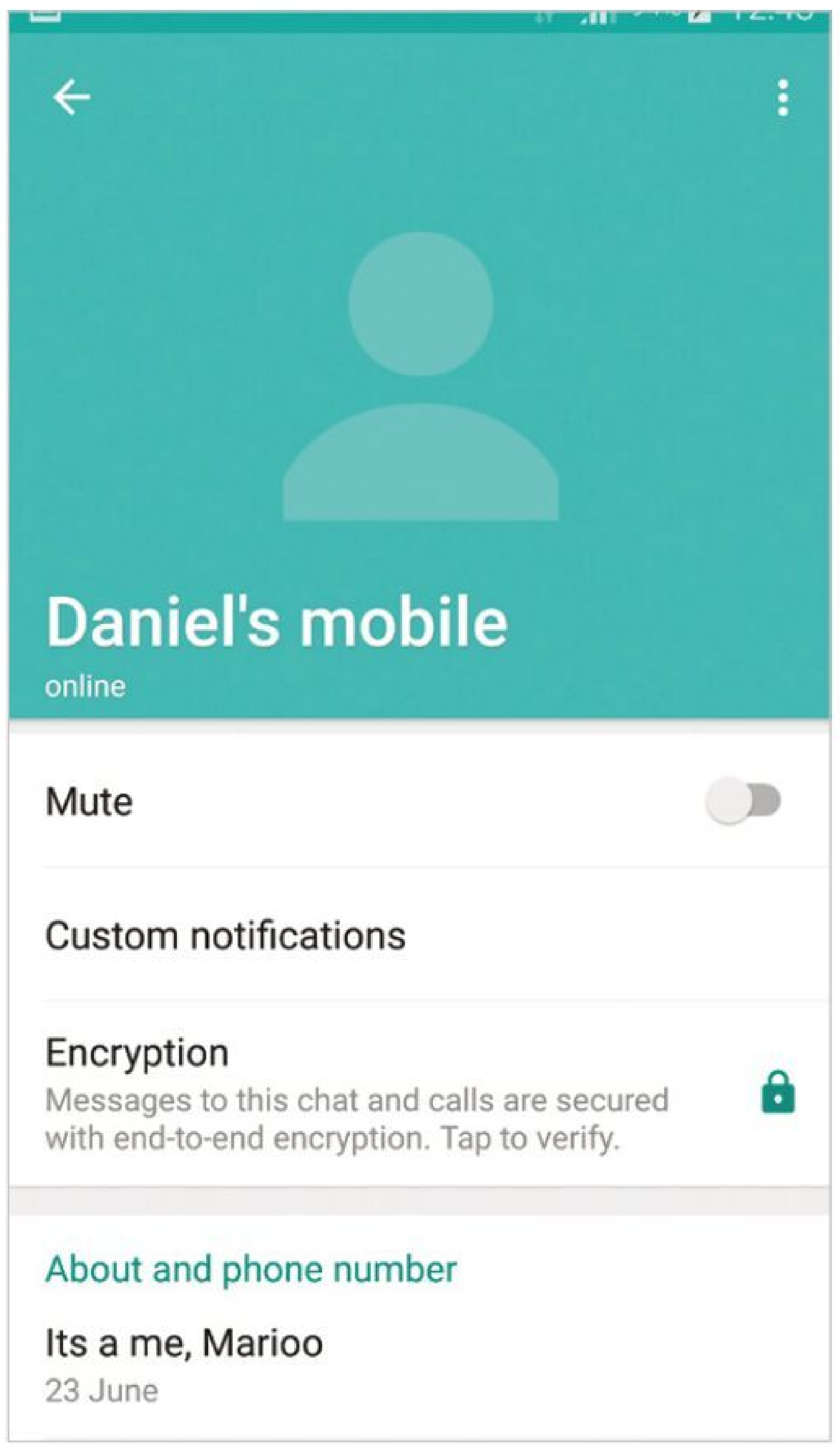
CYBER
BULLYING

Any contacts that send you a message can be blocked, muted and the chat content cleared or emailed if needed. Just open the message, tap the three vertical dots and select the appropriate option from the menu.


94%
12:40
Daniel's mo
online
Messages to this ch
with end-to-end enc
1 UNRE
View contact
Media
Search
Mute
Wallpaper
More

Hi 12:38

Once you have a message open, long tap the contact and you can see the contact's information. From there you're able to block them, report them as a spam user, mute them or even verify that the messages sent are fully encrypted.


Daniel's mobile
online
Mute
Custom notifications
Encryption
About and phone number

Messages to this chat and calls are secured with end-to-end encryption. Tap to verify.

Its a me, Marioo
23 June

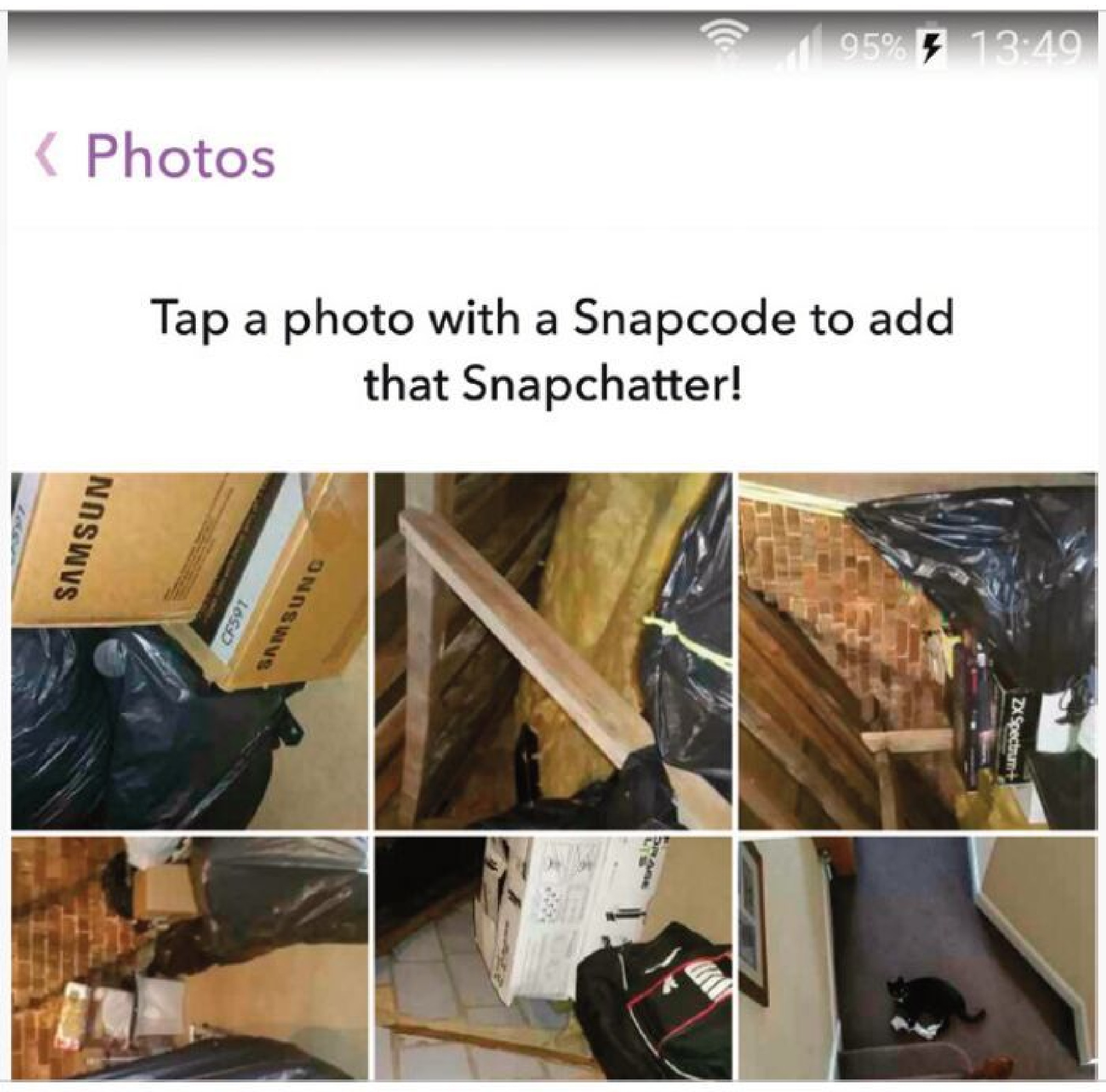
Staying Safe with Snapchat for Teens

Popular amongst young teens, Snapchat has continually raised its appeal by offering alluring features at the cost of security and privacy. The most recent update (at the time of writing) is Snap Maps, a feature that tells everyone where you currently are.

Safety Snaps

Snapchat has some useful features but also some slightly scary security issues. It's best then to make sure that you're as safe as possible when using it.

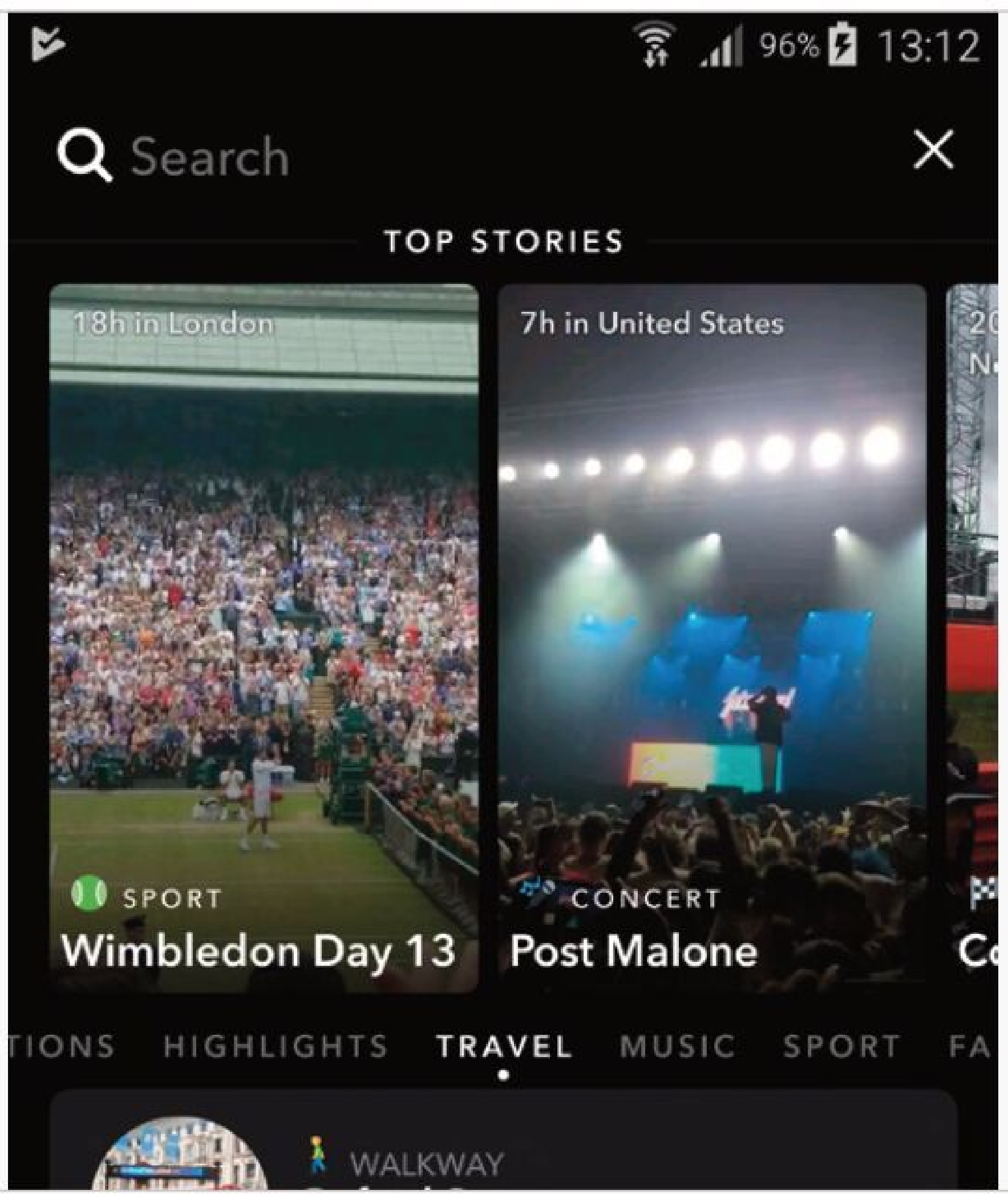
Parents: Take the time to look through your child's Snapchat contacts. Together you can limit who can see what and who can contact your child through Snapchat's various functions.



Photos

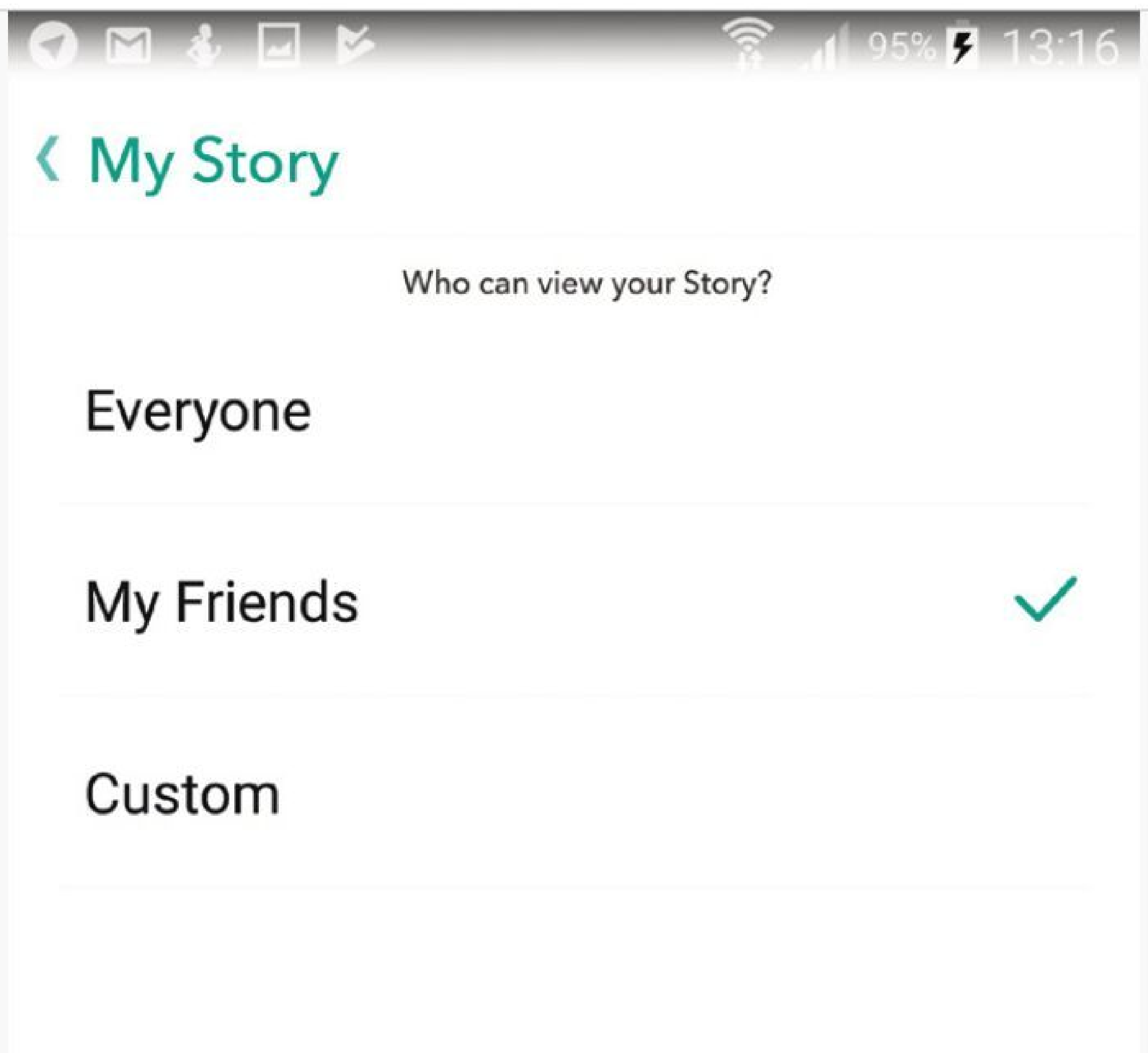
Tap a photo with a Snapcode to add that Snapchatter!

Tapping the magnifying glass icon will open the global Snapchat Top Stories. From there a user can search for something specific or view any Snapchats via the various headings. Be careful here, there's a lot of inappropriate content out there, along with dubious individuals who would like your information.



96% 13:12
Search
TOP STORIES
18h in London
7h in United States
SPORT
Wimbledon Day 13
CONCERT
Post Malone
TIONS HIGHLIGHTS TRAVEL MUSIC SPORT FA
WALKWAY

You can create your own Snapchat Stories, by tapping the three dots in a triangle in the bottom right of the Snapchat interface. Make sure that you also tap the cog icon in the top right within Stories, in here you'll be able to limit who sees your stories. Try and avoid choosing Everyone, if possible.



My Story

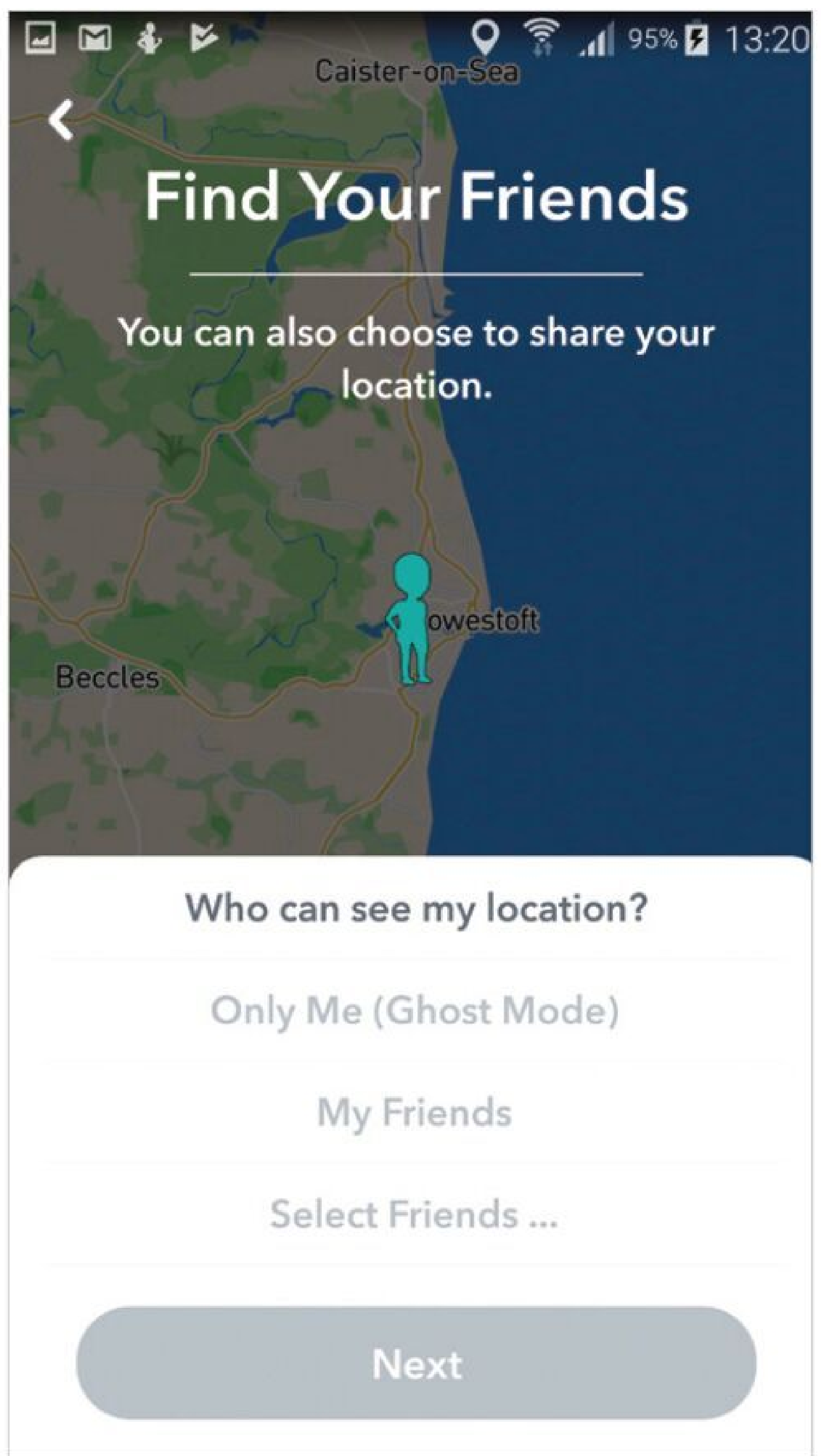
Who can view your Story?

Everyone

My Friends ✓

Custom

Snap Maps is the newest feature to Snapchat, one that enables other Snapchat users to see where you are in the world. To open it, pinch your fingers like you're zooming out from the camera screen. When asked, you're able to set who can see your location. Always ensure you know your friends, or enable Ghost mode for better privacy.



Find Your Friends

You can also choose to share your location.

Who can see my location?

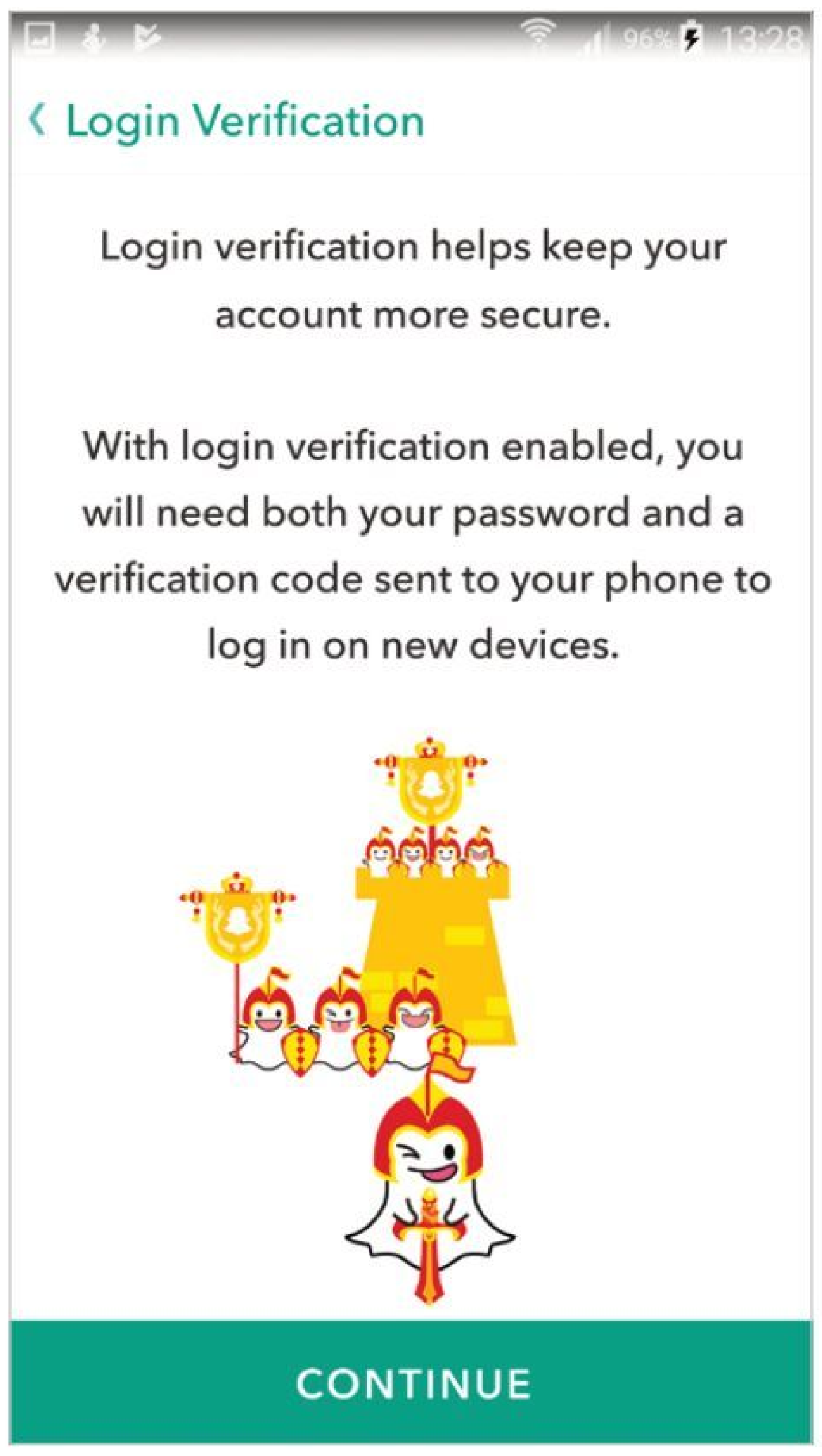
Only Me (Ghost Mode)

My Friends

Select Friends ...

95% 13:20
Caister-on-Sea
Lowestoft
Beccles
Next

Tap on the Snapchat icon, followed by the cog in the top right to access your account settings. Scroll down a little way to Login Verification and tap it. This is a two-step authentication process that requires both a code sent to your device, as well as your login details to open Snapchat. Useful if you ever lose your device.



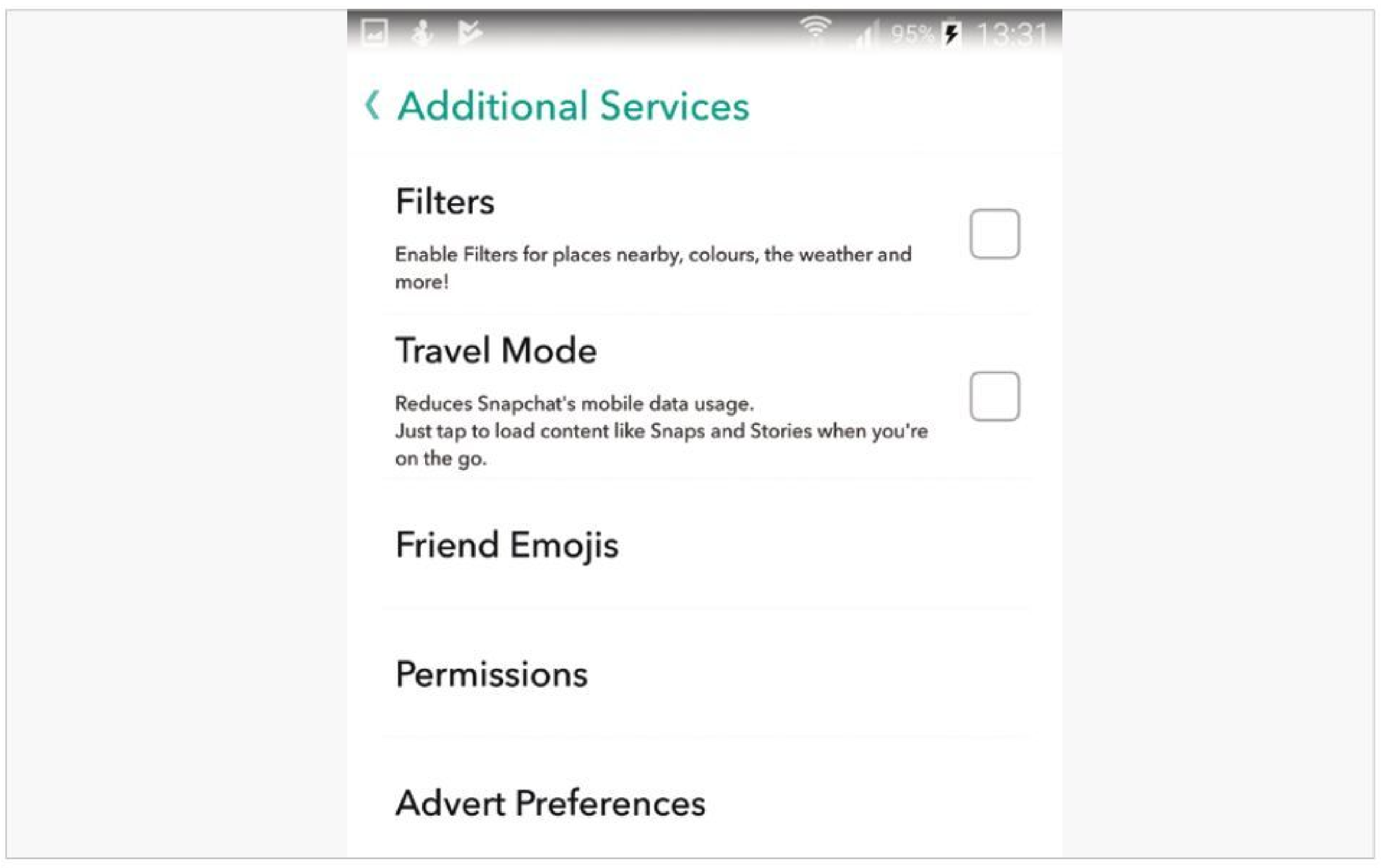
95% 13:28

‹ Login Verification

Login verification helps keep your account more secure.

With login verification enabled, you will need both your password and a verification code sent to your phone to log in on new devices.

Whilst still in the account settings, scroll down to Manage Preferences under the Additional Services heading. In here you can limit the mobile data use and enable filters for nearby places, change the app permissions and advert preferences.



95% 13:31

‹ Additional Services

Filters ☐
Enable Filters for places nearby, colours, the weather and more!

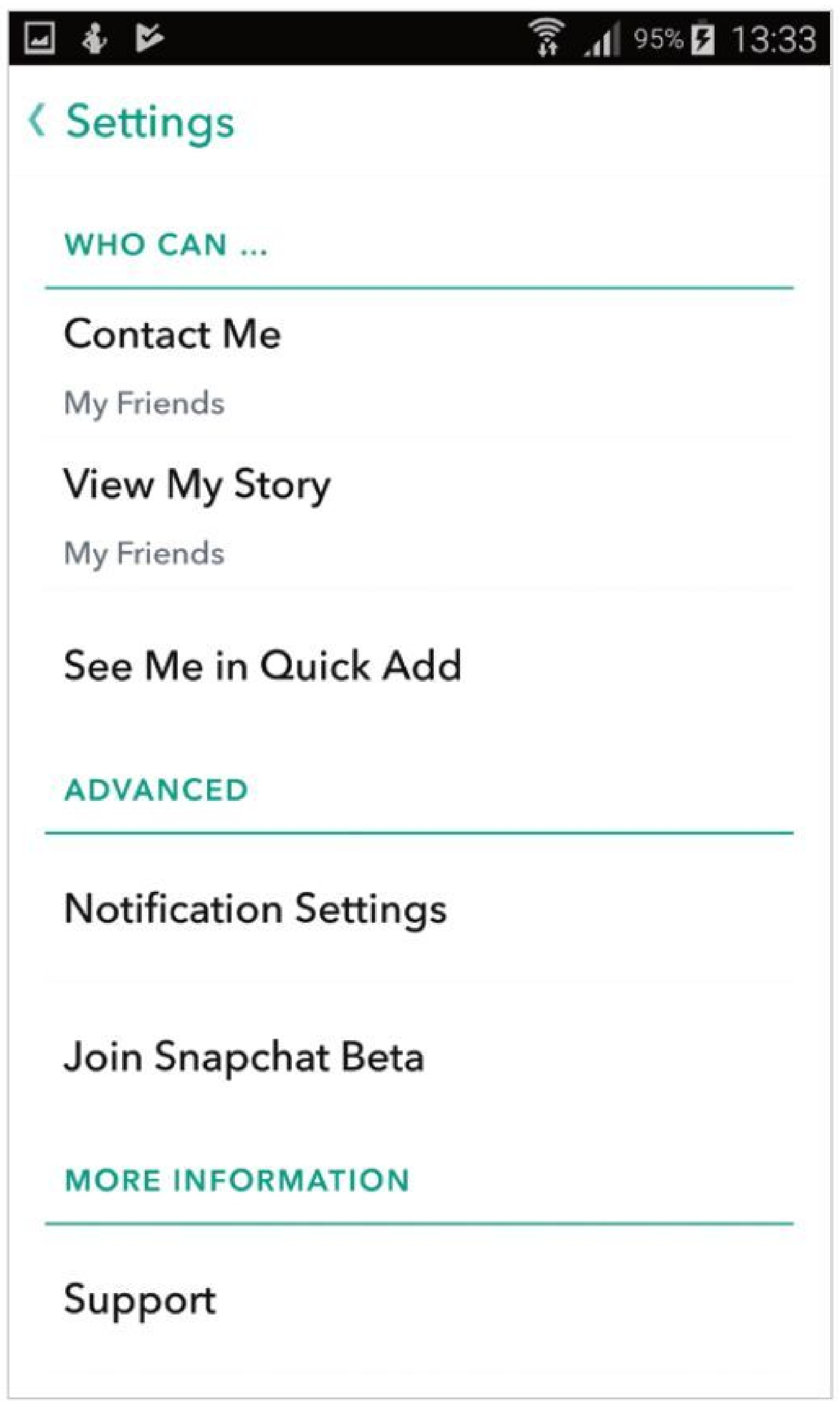
Travel Mode ☐
Reduces Snapchat's mobile data usage.
Just tap to load content like Snaps and Stories when you're on the go.

Friend Emojis

Permissions

Advert Preferences

Under the Additional Services heading, the Who Can… heading enables you to specify who can contact you or see your Stories. It's best to limit your account so only friends are able to see you or any posts you make, as opposed to the Everyone option.



95% 13:33

‹ Settings

WHO CAN ...

Contact Me
My Friends

View My Story
My Friends

See Me in Quick Add

ADVANCED

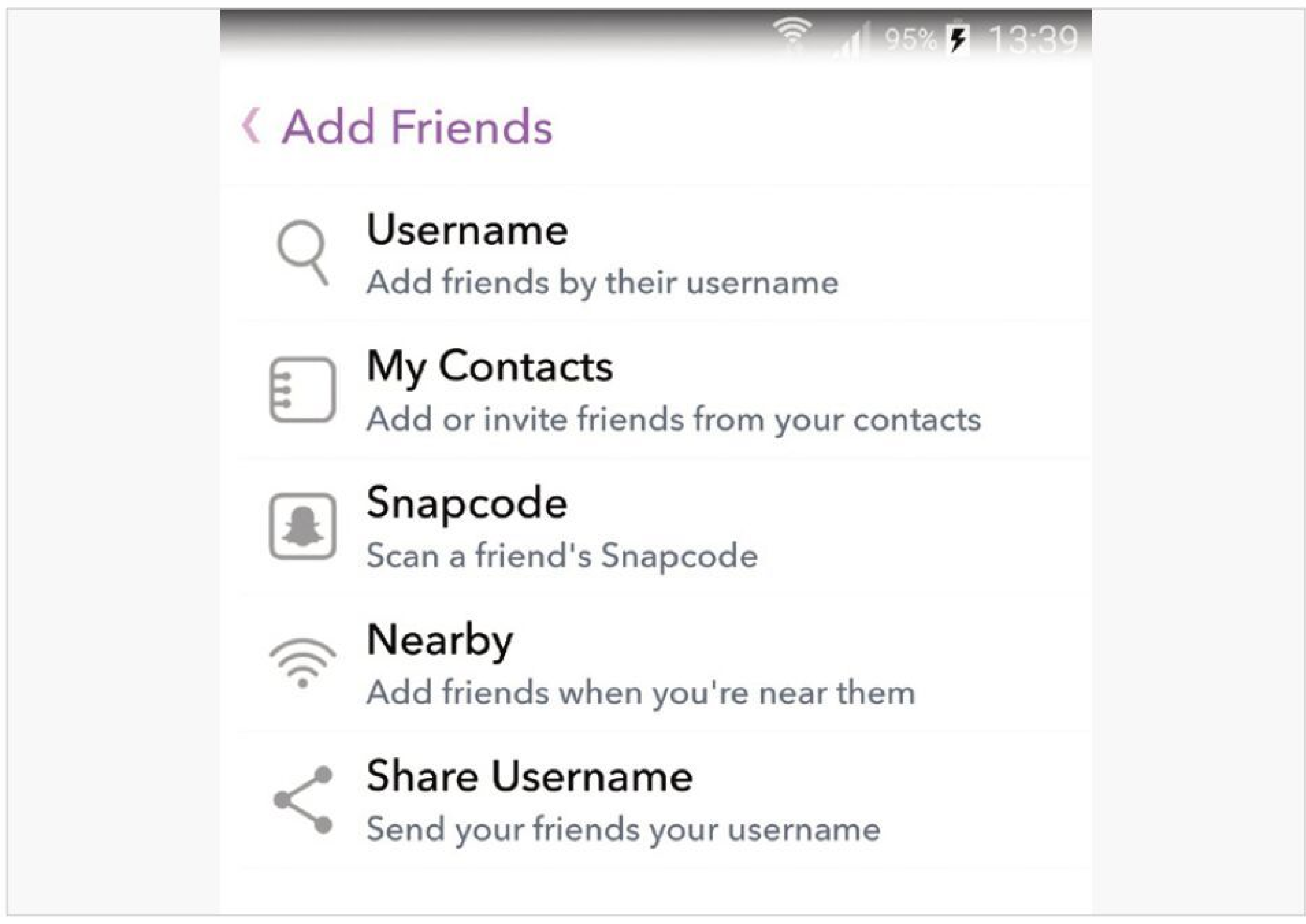
Notification Settings

Join Snapchat Beta

MORE INFORMATION

Support

Be wary of the Add Friends function in Snapchat. From it you can add friends in your contacts list, any that have sent you their Snapcode, shared friends lists, or you can opt to locate other Snapchat users based on whether they're nearby. Obviously this is a privacy and security concern, so be aware of it.



95% 13:39

‹ Add Friends

Username
Add friends by their username

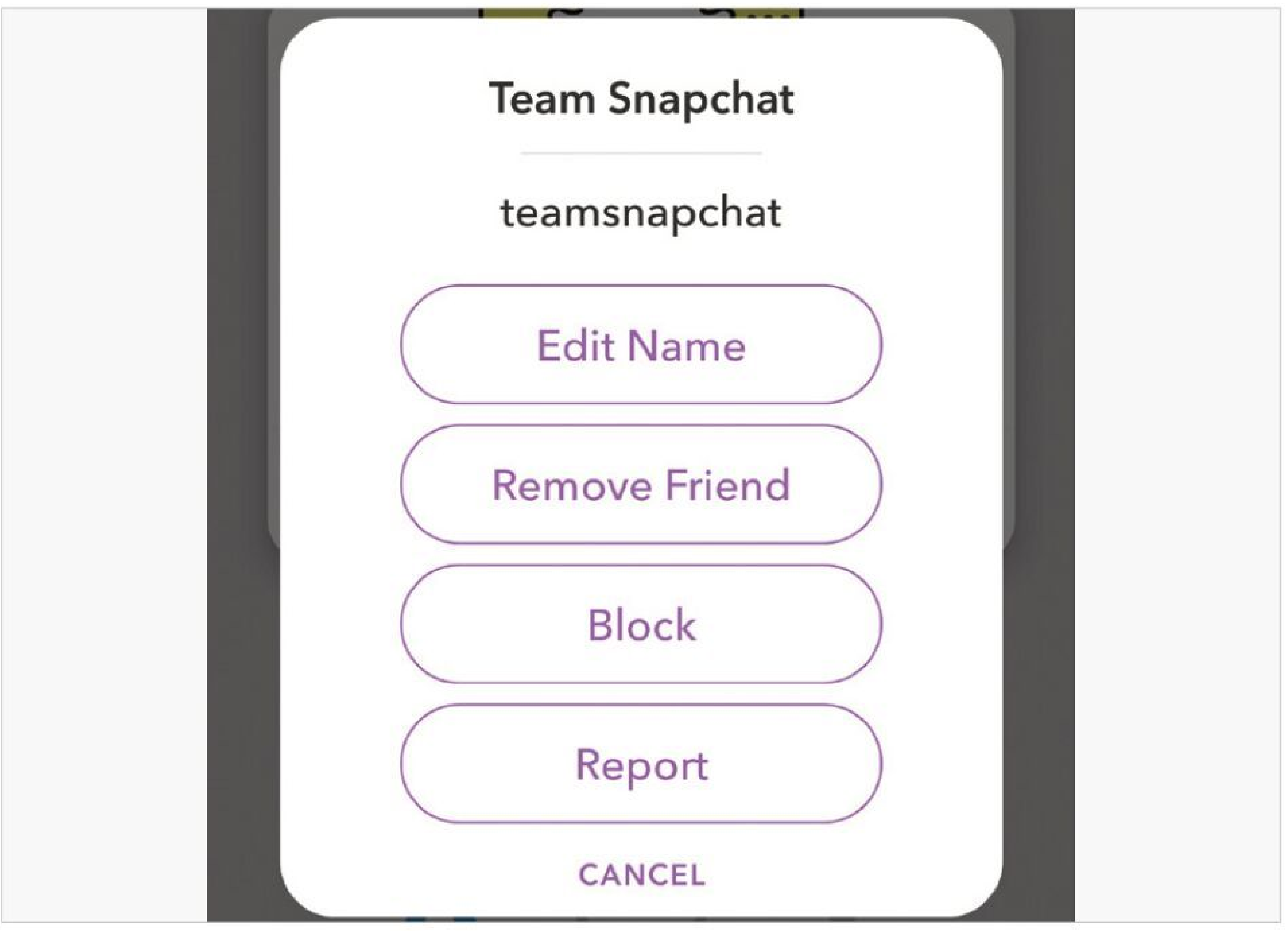
My Contacts
Add or invite friends from your contacts

Snapcode
Scan a friend's Snapcode

Nearby
Add friends when you're near them

Share Username
Send your friends your username

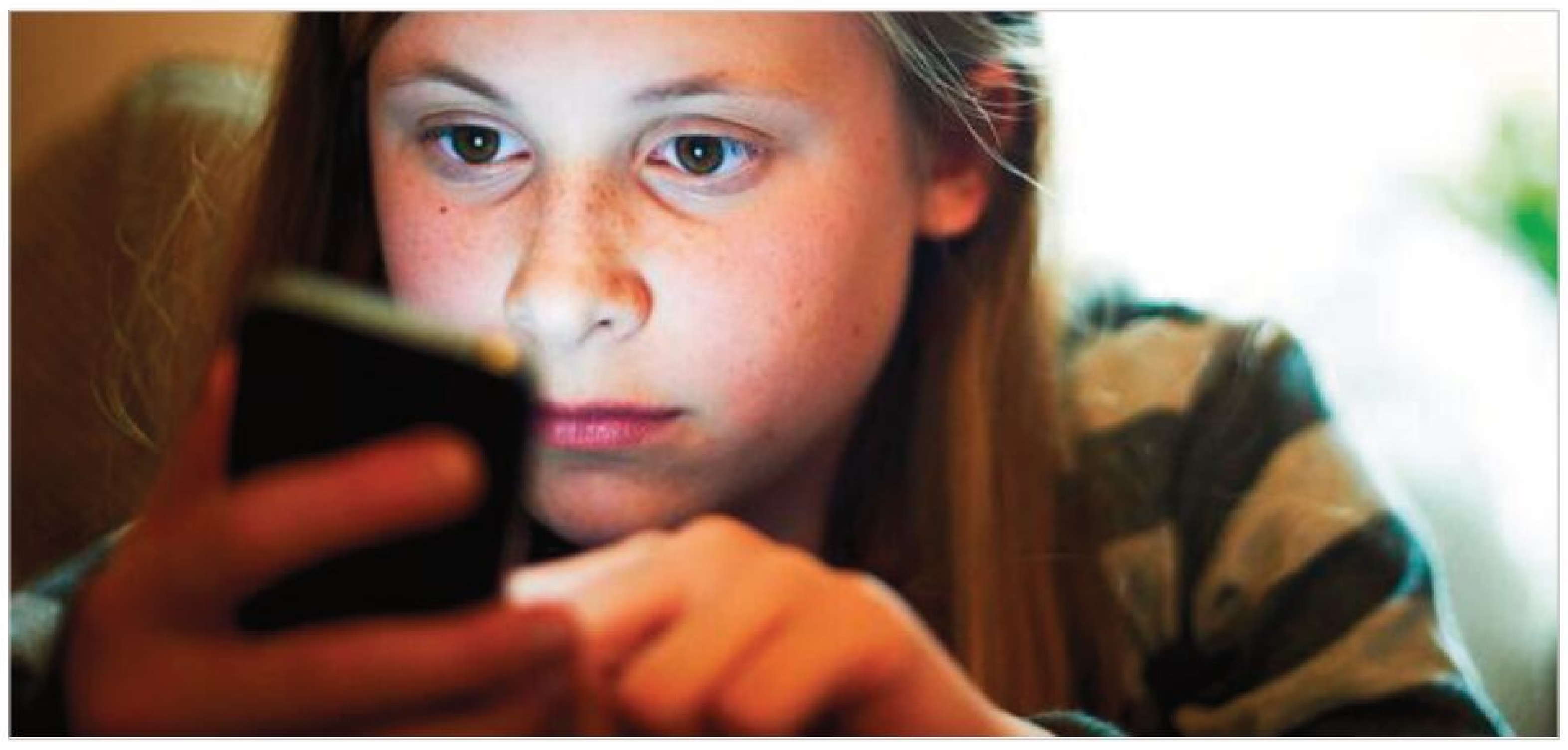
You can easily remove friends, block and report other Snapchat users by long pressing the contact or Snapchat feed and selecting the option from the menu. Make sure you've taken any screenshots of inappropriate content before blocking, to use as proof if reporting the contact.



Team Snapchat

teamsnapchat

Just as with all social media platforms, if you're uncomfortable with the content or messages that someone is sending you, tell a parent, guardian, teacher or other responsible adult. Don't respond, don't send anything to them and always think before posting any images of yourself and your location.



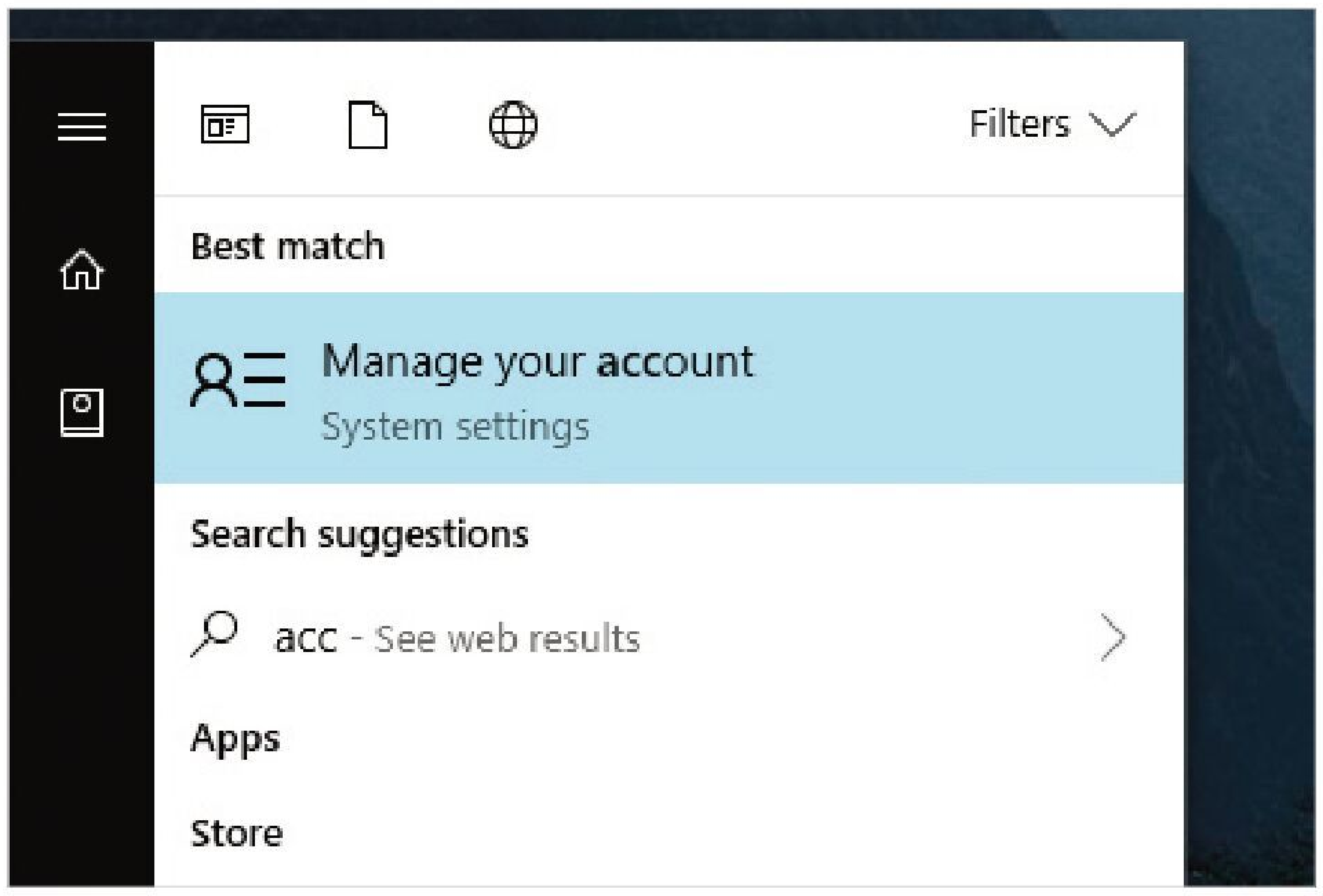
Creating a Child Account in Windows 10

If you're sharing a Windows 10 computer with your children, or they have one for themselves, then setting them up with their own account will work better for you both in the long run. A Windows 10 child's account gives them freedom, and you can set up certain restrictions.

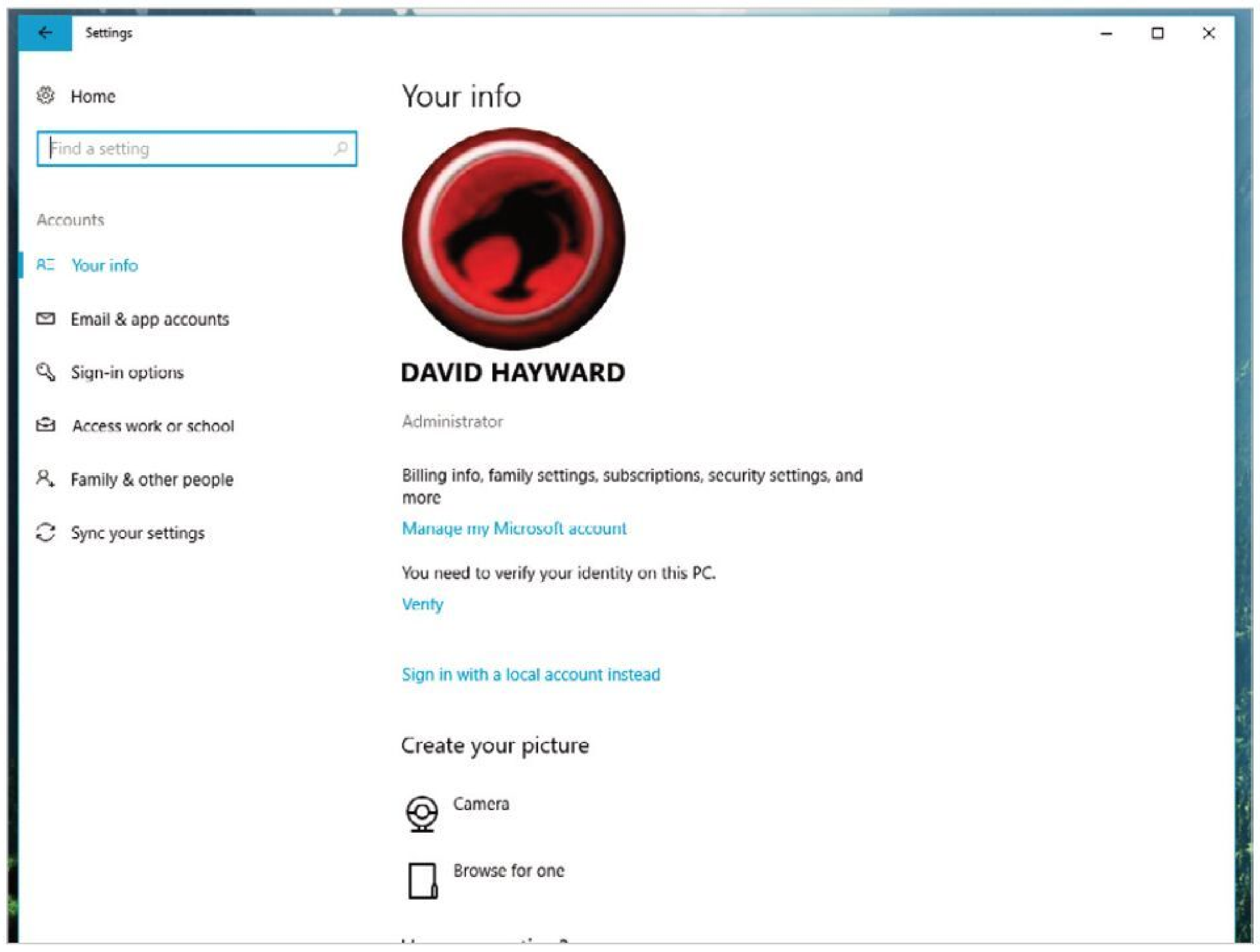
Windows 10 for Children

With a Windows 10 child account you're able to set up age restrictions, time limits and ensure they're not visiting sites or using apps they shouldn't.

STEP 1 Start off by clicking the Windows Start button and typing 'account'. The first result that should appear is Manage your account, if anything else appears, maybe you have some work labelled 'account', then scroll down until you find the Manage your account option.


Filters
Best match
Manage your account
System settings
Search suggestions
acc - See web results
Apps
Store

STEP 2 You now find yourself at the Windows 10 Settings page, in the Accounts section portal. Notice there are links down the left-hand side, look for the Family & Other People link and click it to continue with the process.


Settings
Home
Find a setting
Accounts
Your info
Email & app accounts
Sign-in options
Access work or school
Family & other people
Sync your settings
Your info
DAVID HAYWARD
Administrator

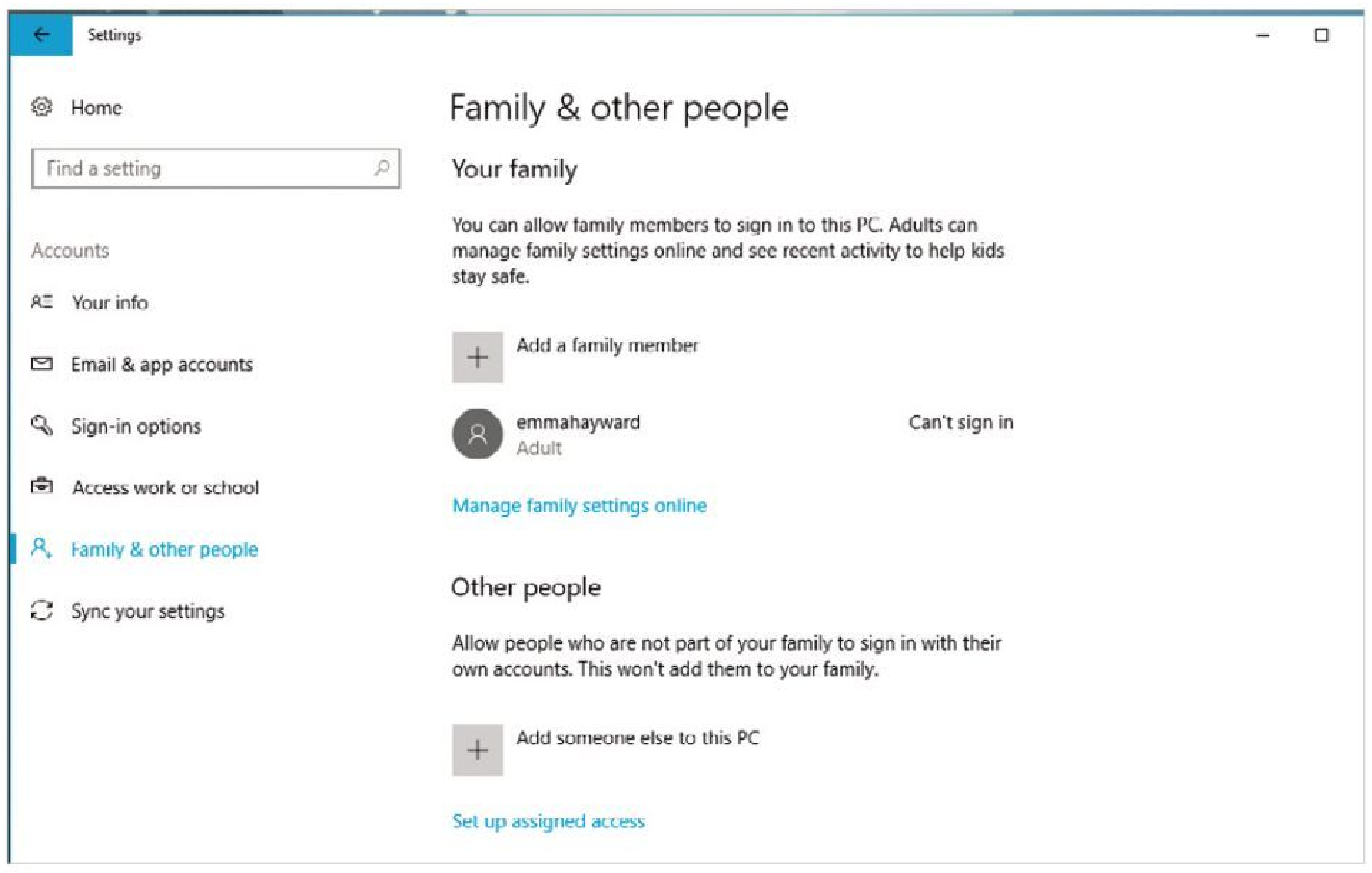
Billing info, family settings, subscriptions, security settings, and more

Manage my Microsoft account

You need to verify your identity on this PC.

Verify
Sign in with a local account instead
Create your picture
Camera
Browse for one

STEP 3 You need to sign in with a Microsoft account for this to work. If you've not already set up a main Microsoft login account for Windows, you'll need to click the Sign in with a Microsoft account option. Once done, you're presented with the current family members who already have MS accounts.


Settings
Home
Find a setting
Accounts
Your info
Email & app accounts
Sign-in options
Access work or school
Family & other people
Sync your settings
Family & other people
Your family

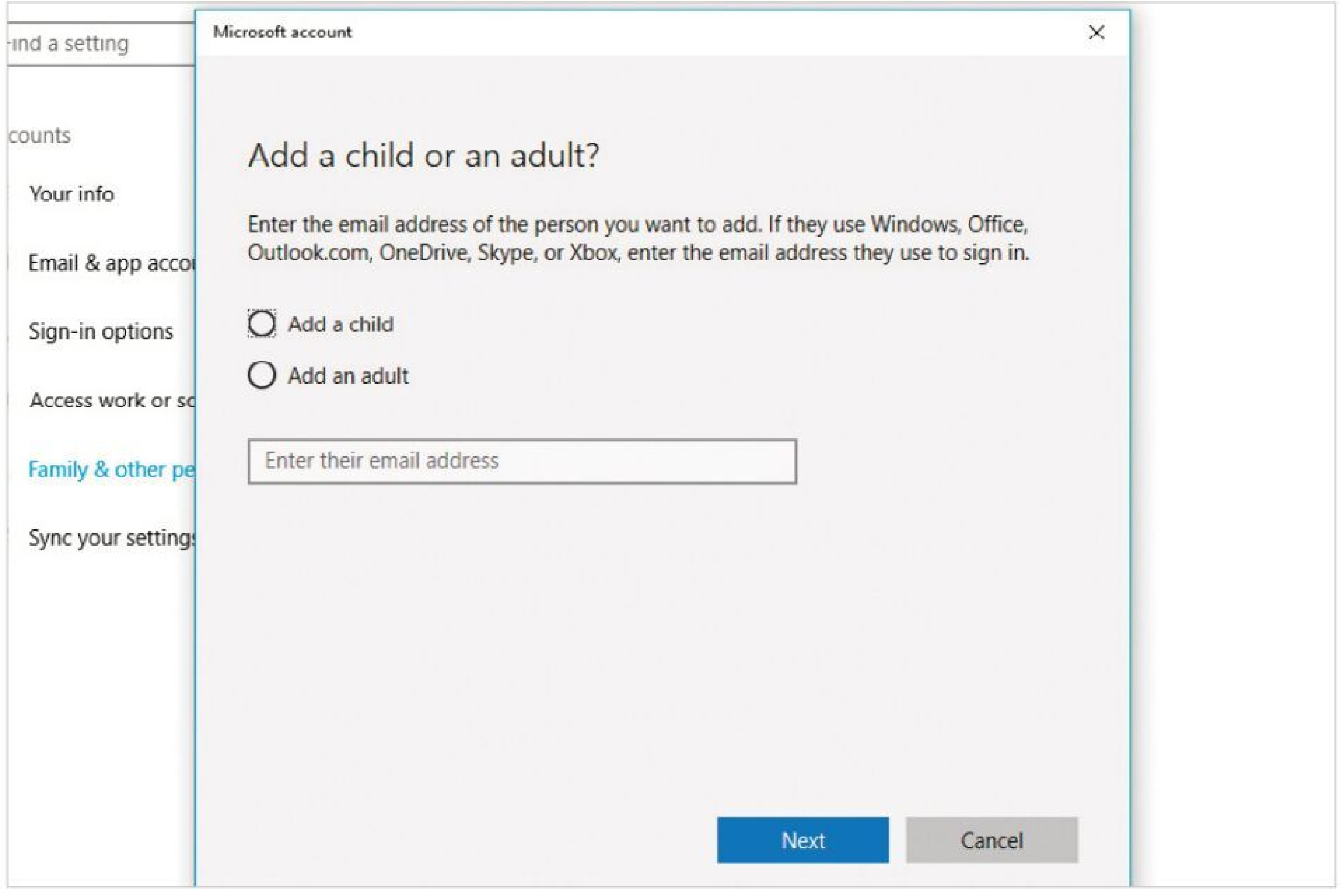
You can allow family members to sign in to this PC. Adults can manage family settings online and see recent activity to help kids stay safe.

Add a family member
emmahayward
Adult
Can't sign in
Manage family settings online
Other people

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

Add someone else to this PC
Set up assigned access

STEP 4 Next click on the Add a Family Member link, next to the plus sign under the Your Family section. This will launch a new pop-up window to create a new Microsoft account. You need to make sure that your child has an email address and that you or they currently have access to it to authenticate the process.

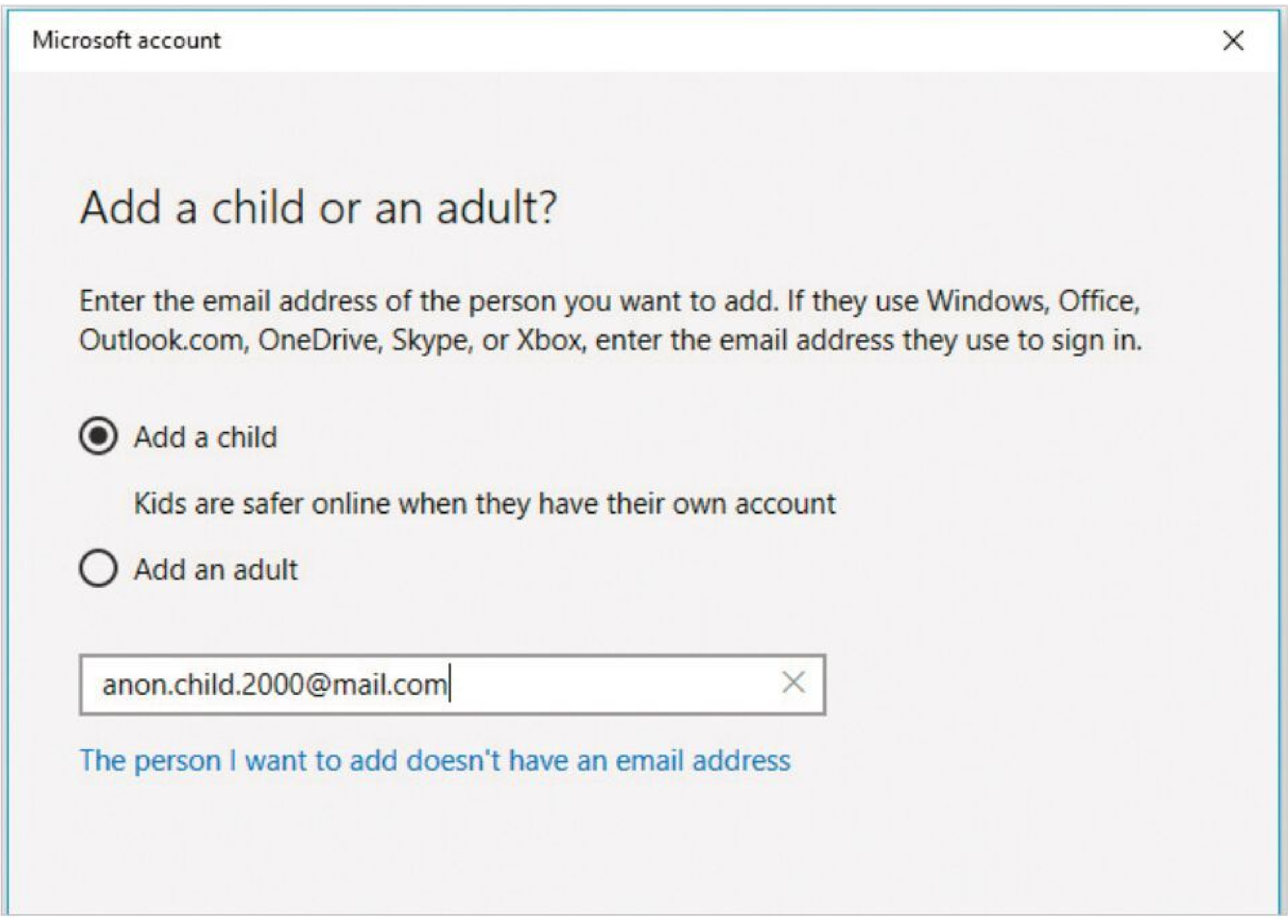

Microsoft account
Add a child or an adult?

Enter the email address of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email address they use to sign in.

○ Add a child
○ Add an adult

Enter their email address
Next
Cancel

STEP 5 Click the Add a Child option in the new account window and enter their email in the text box section below. When you're ready, click on the Next button.



Microsoft account

Add a child or an adult?

Enter the email address of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email address they use to sign in.

● Add a child

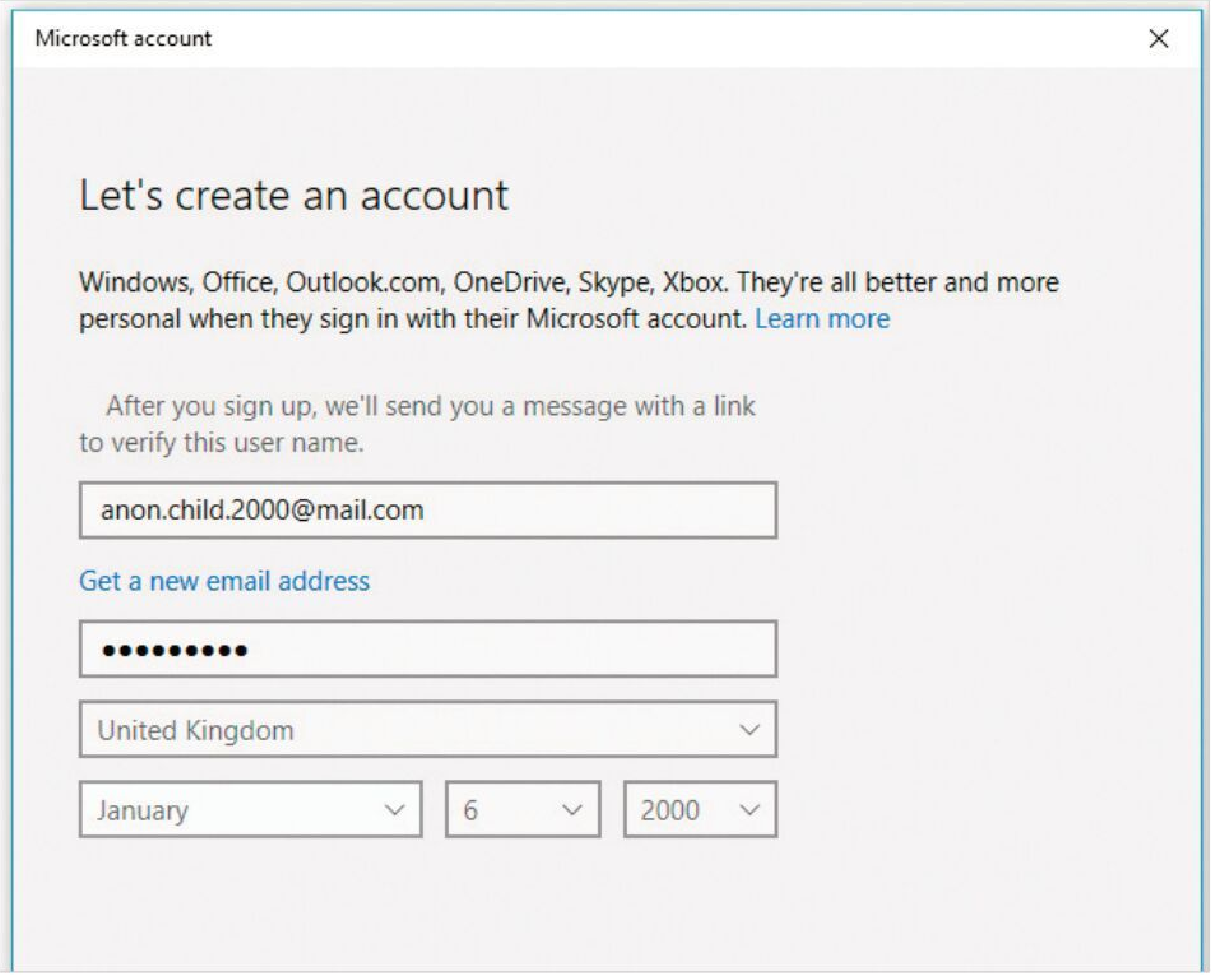
Kids are safer online when they have their own account

○ Add an adult

anon.child.2000@mail.com

The person I want to add doesn't have an email address

STEP 6 You now get the message that it's not a Microsoft account, click the link to Create a Microsoft Account. This will bring you to a new window with the email address you've entered already filled in. Complete the relevant details and click the Next button to continue.



Microsoft account

Let's create an account

Windows, Office, Outlook.com, OneDrive, Skype, Xbox. They're all better and more personal when they sign in with their Microsoft account. Learn more

After you sign up, we'll send you a message with a link to verify this user name.

anon.child.2000@mail.com

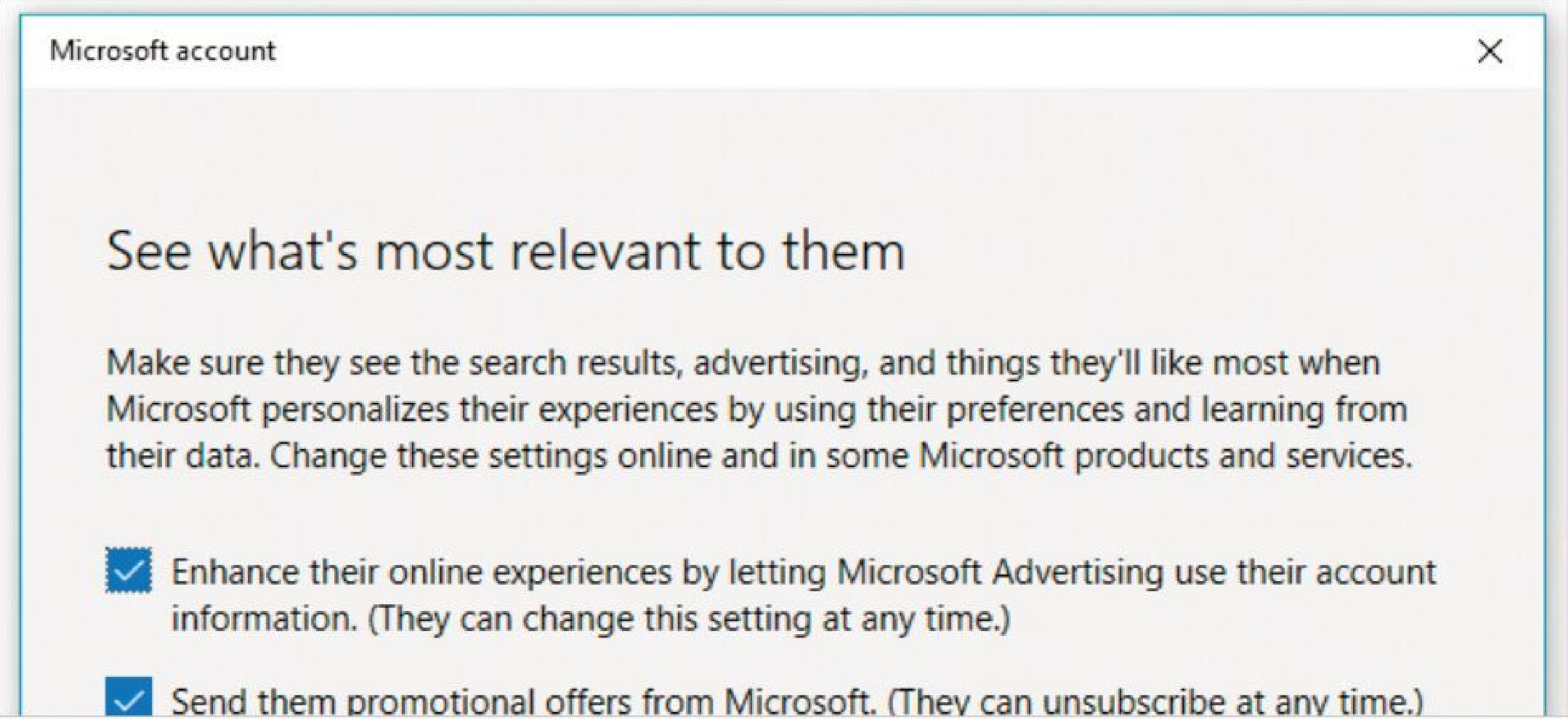
Get a new email address

••••••••••

United Kingdom

January 6 2000

STEP 7 The next section details what level of search and advertising Microsoft will allow to the account. Obviously you can untick both boxes or leave them as they are, it all depends on what you want. However, for the sake of enhanced privacy, we recommend unticking both. Click Next when you're ready.



Microsoft account

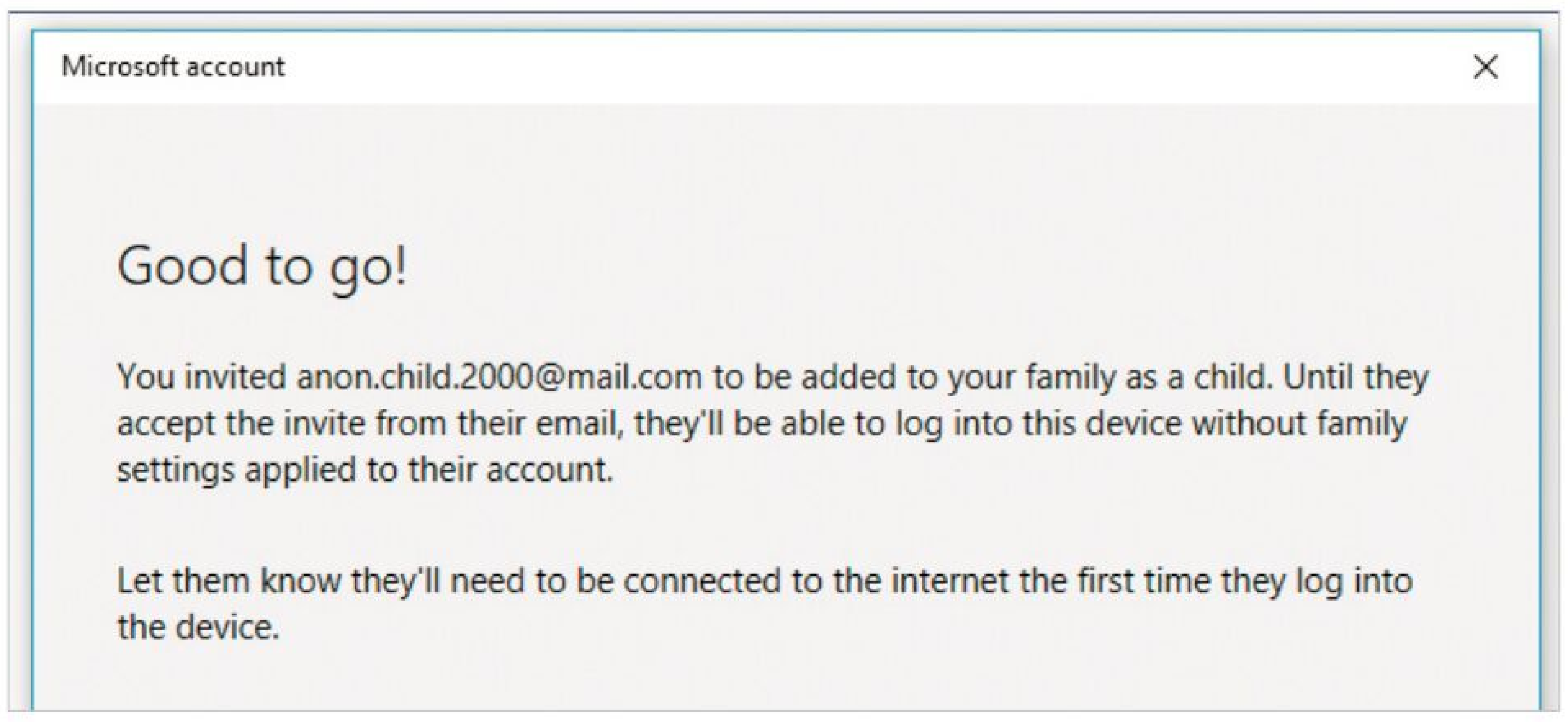
See what's most relevant to them

Make sure they see the search results, advertising, and things they'll like most when Microsoft personalizes their experiences by using their preferences and learning from their data. Change these settings online and in some Microsoft products and services.

☑ Enhance their online experiences by letting Microsoft Advertising use their account information. (They can change this setting at any time.)

☑ Send them promotional offers from Microsoft. (They can unsubscribe at any time.)

STEP 8 The child's account is now ready to be activated. The message box informs you that you need to respond to the email Microsoft has sent before they're able to login in to the Windows 10 computer. Click the Close button when you're ready.



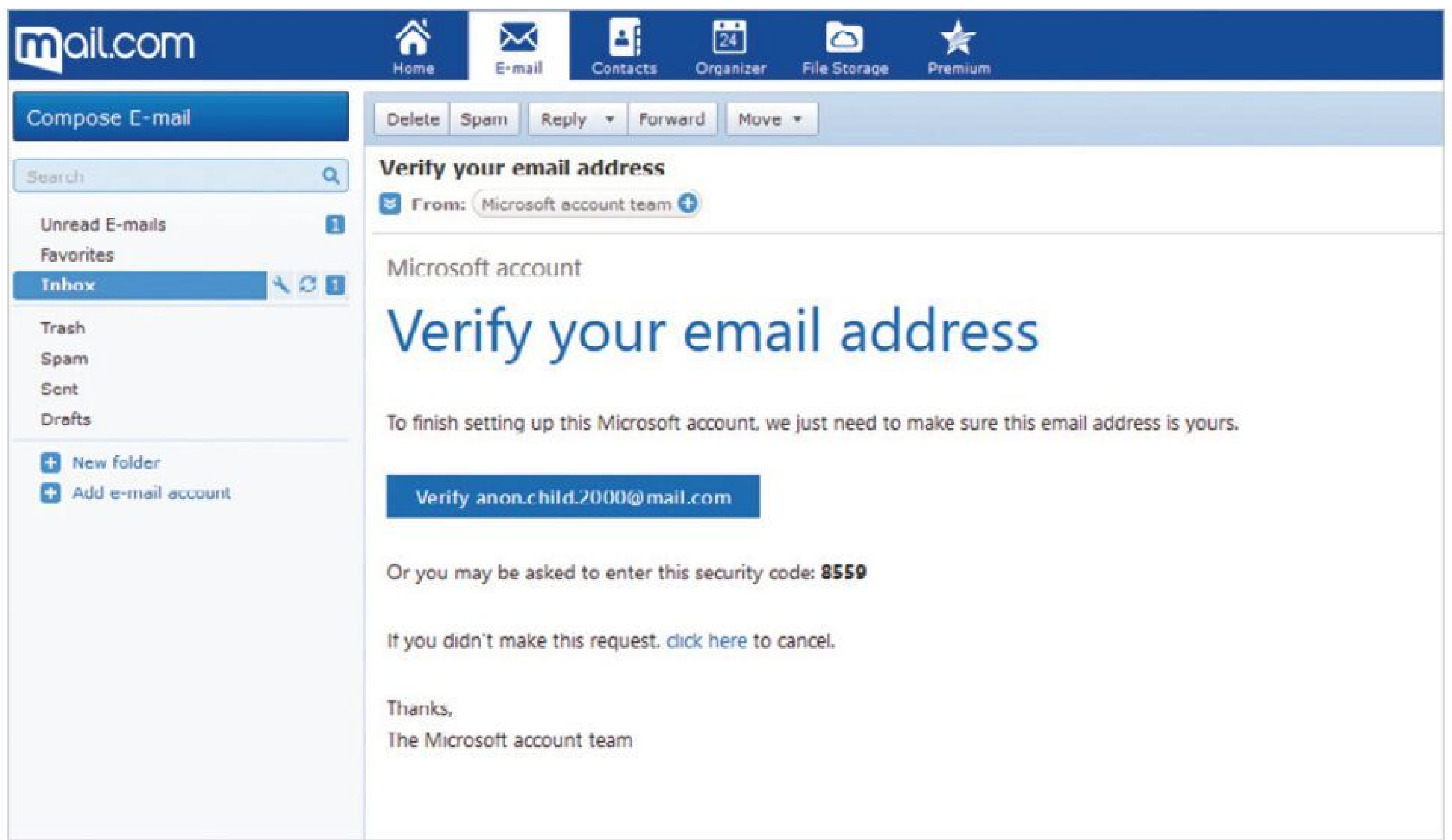
Microsoft account

Good to go!

You invited anon.child.2000@mail.com to be added to your family as a child. Until they accept the invite from their email, they'll be able to log into this device without family settings applied to their account.

Let them know they'll need to be connected to the internet the first time they log into the device.

STEP 9 Microsoft will send some emails to the child's account. One will be a Verification email, and you, or your child, will need to click the link to activate the account; they need to login to Microsoft online to complete the process. The other email will be an invitation to join the family account, which you also need to Accept.



Verify your email address

From: Microsoft account team

Microsoft account

Verify your email address

To finish setting up this Microsoft account, we just need to make sure this email address is yours.

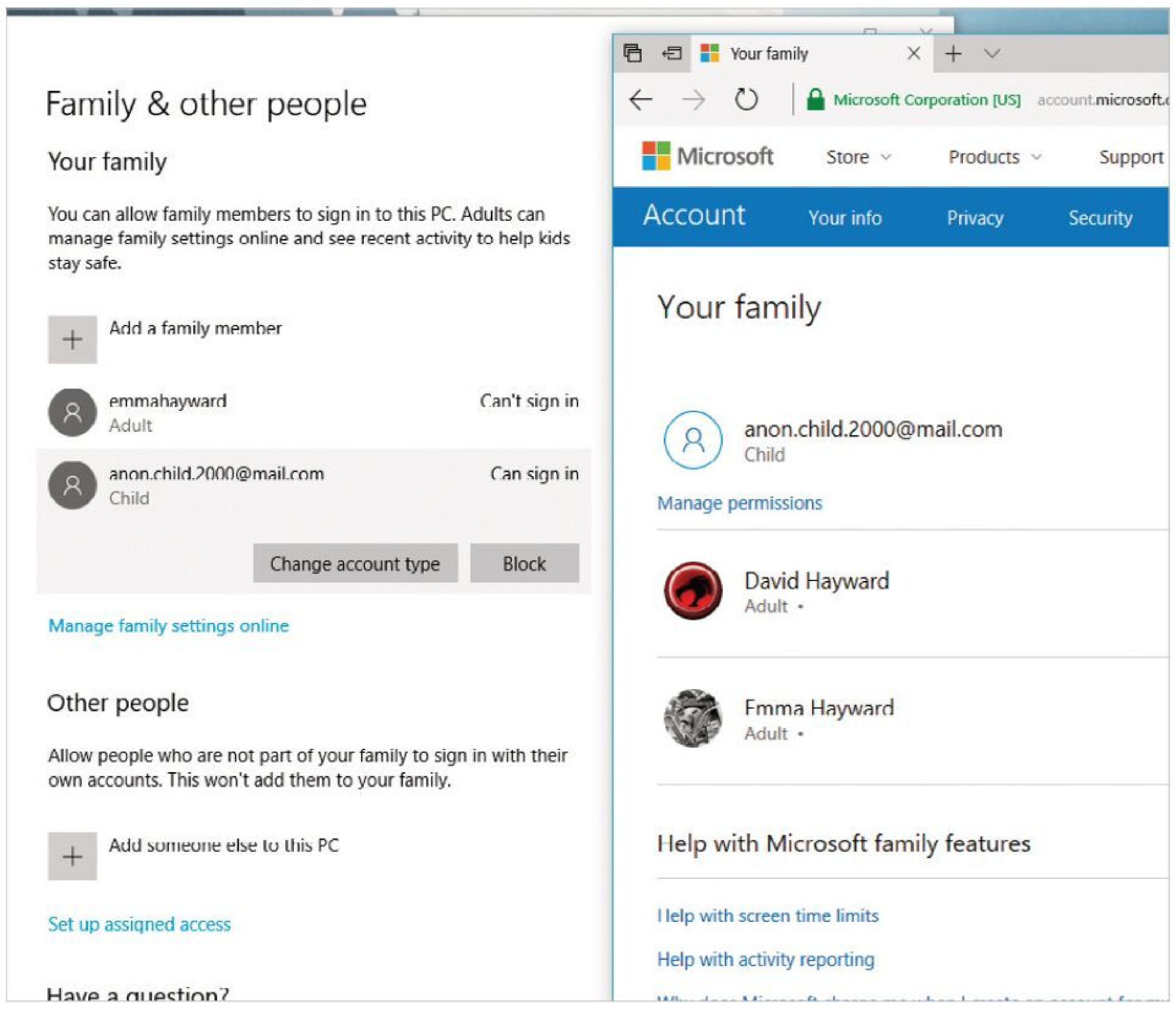
Verify anon.child.2000@mail.com

Or you may be asked to enter this security code: **8559**

If you didn't make this request, click here to cancel.

Thanks,
The Microsoft account team

STEP 10 Using the child account to join the family will send emails to you confirming the accepted invitation. Back at the Windows 10 Family & Other People window, you can now click the child's account and allow it to login, or manage it via the Microsoft Family portal online, which we'll look at in the next tutorial.



Family & other people

Your family

You can allow family members to sign in to this PC. Adults can manage family settings online and see recent activity to help kids stay safe.

Add a family member

emmahayward — Adult — Can't sign in

anon.child.2000@mail.com — Child — Can sign in

Change account type | Block

Manage family settings online

Other people

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

Add someone else to this PC

Set up assigned access

Have a question?

Your family

anon.child.2000@mail.com
Child

Manage permissions

David Hayward
Adult

Emma Hayward
Adult

Help with Microsoft family features

Help with screen time limits

Help with activity reporting

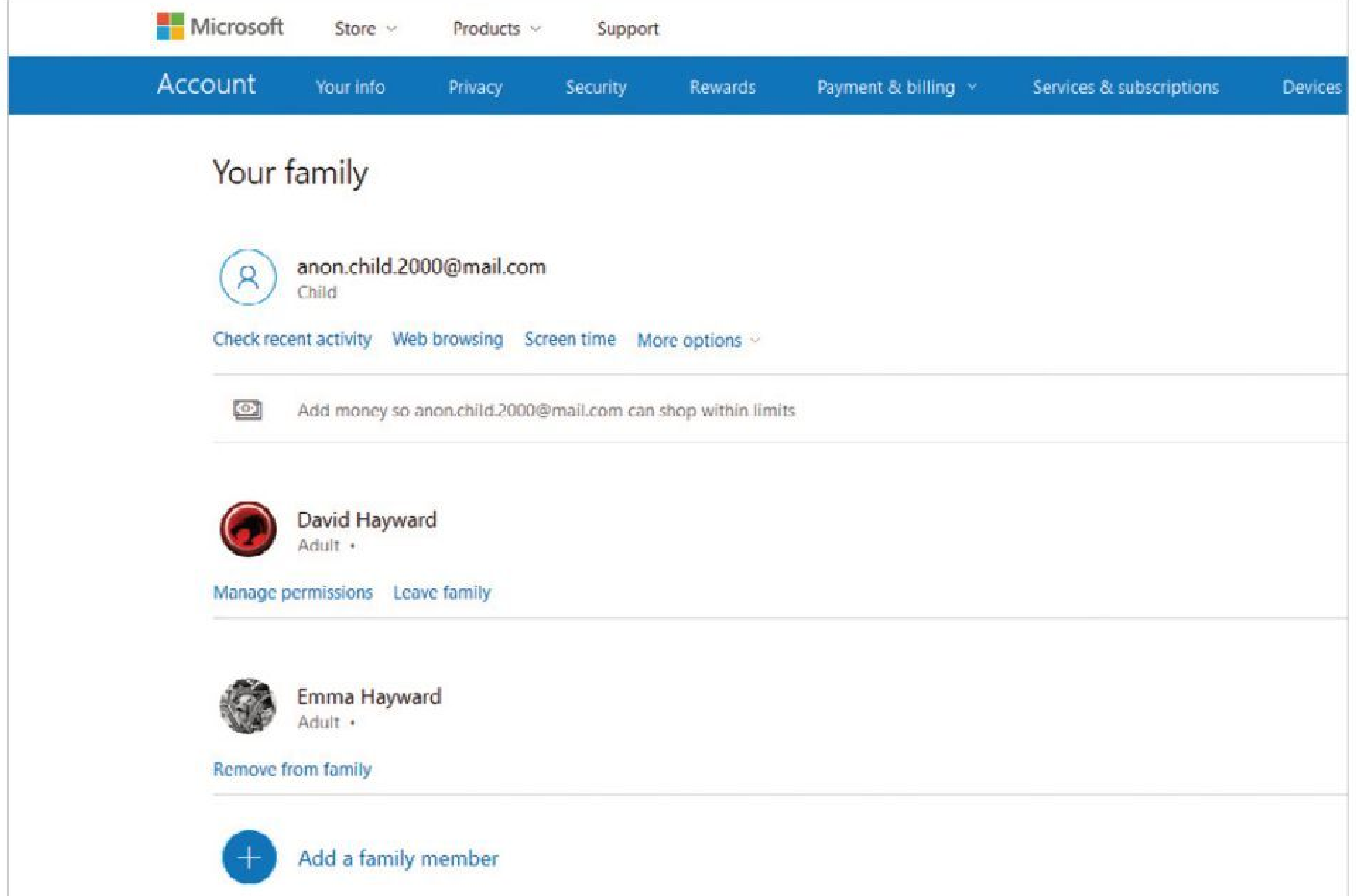
Windows 10 Family Features

Microsoft's Family portal is a continually updating service that allows you to monitor, control and share features across Windows machines and Xbox consoles. It's designed to help share calendars, set screen times for games and set up safe browsing.

Happy Families

The Microsoft Family portal is where you're able to set the various features. First, you need to browse to https://account.microsoft.com to login with your MS account.

STEP 1 When you've logged in to the Microsoft account online, click on the Family link found along the top set of menu options. This will display the current members of your Microsoft account, adults and any children you've added, as per the previous tutorial.


Microsoft
Store
Products
Support
Account
Your info
Privacy
Security
Rewards
Payment & billing
Services & subscriptions
Devices

Your family

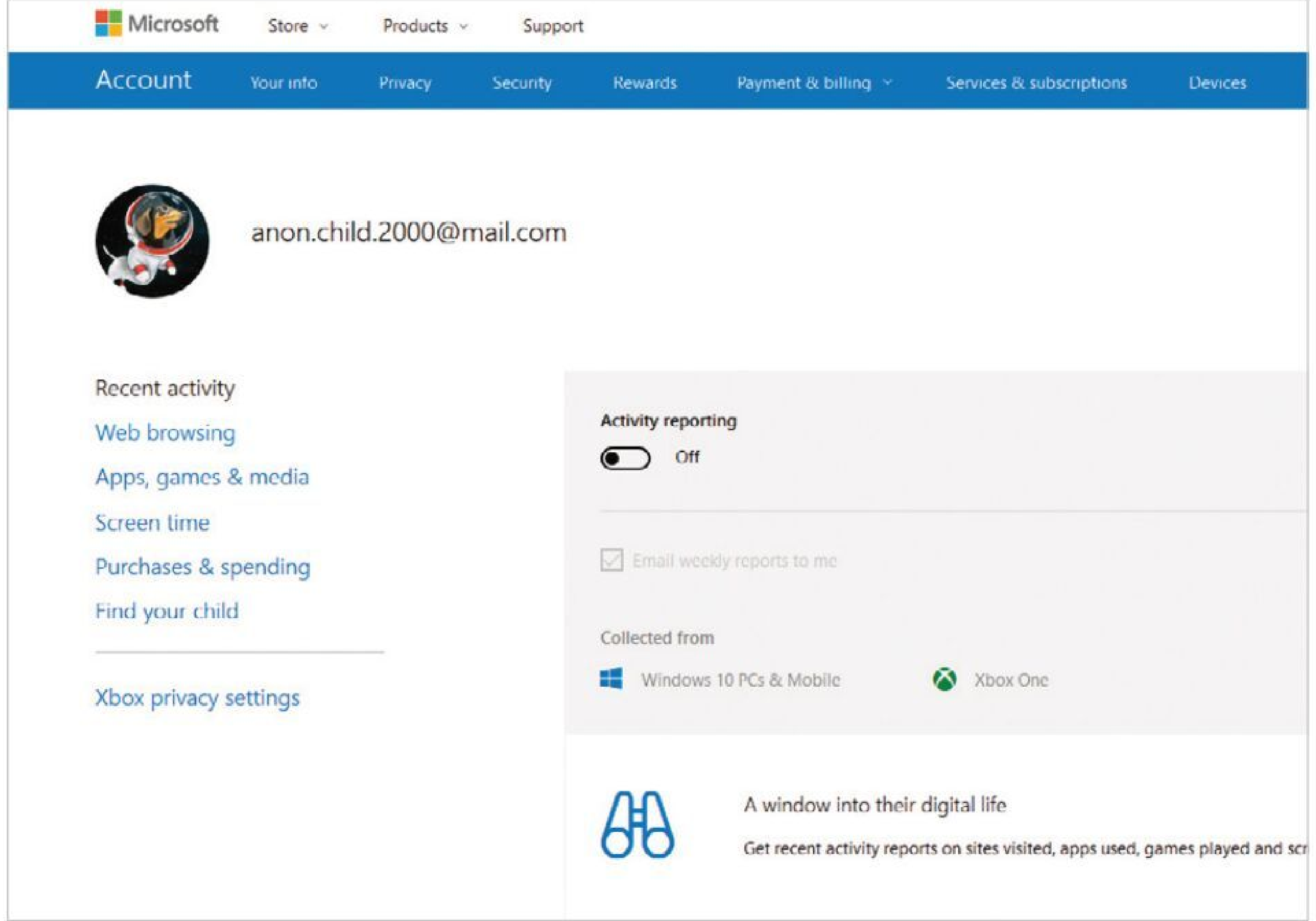
anon.child.2000@mail.com
Child
Check recent activity
Web browsing
Screen time
More options

Add money so anon.child.2000@mail.com can shop within limits

David Hayward
Adult •
Manage permissions
Leave family

Emma Hayward
Adult •
Remove from family
Add a family member

STEP 2 Under the child account you can see four options: Check recent activity, Web browsing, Screen time and More options. All the options can be accessed by clicking on any of the links, so to begin with, click the Check recent activity option.


Microsoft
Store
Products
Support
Account
Your info
Privacy
Security
Rewards
Payment & billing
Services & subscriptions
Devices

anon.child.2000@mail.com

Recent activity
Web browsing
Apps, games & media
Screen time
Purchases & spending
Find your child
Xbox privacy settings

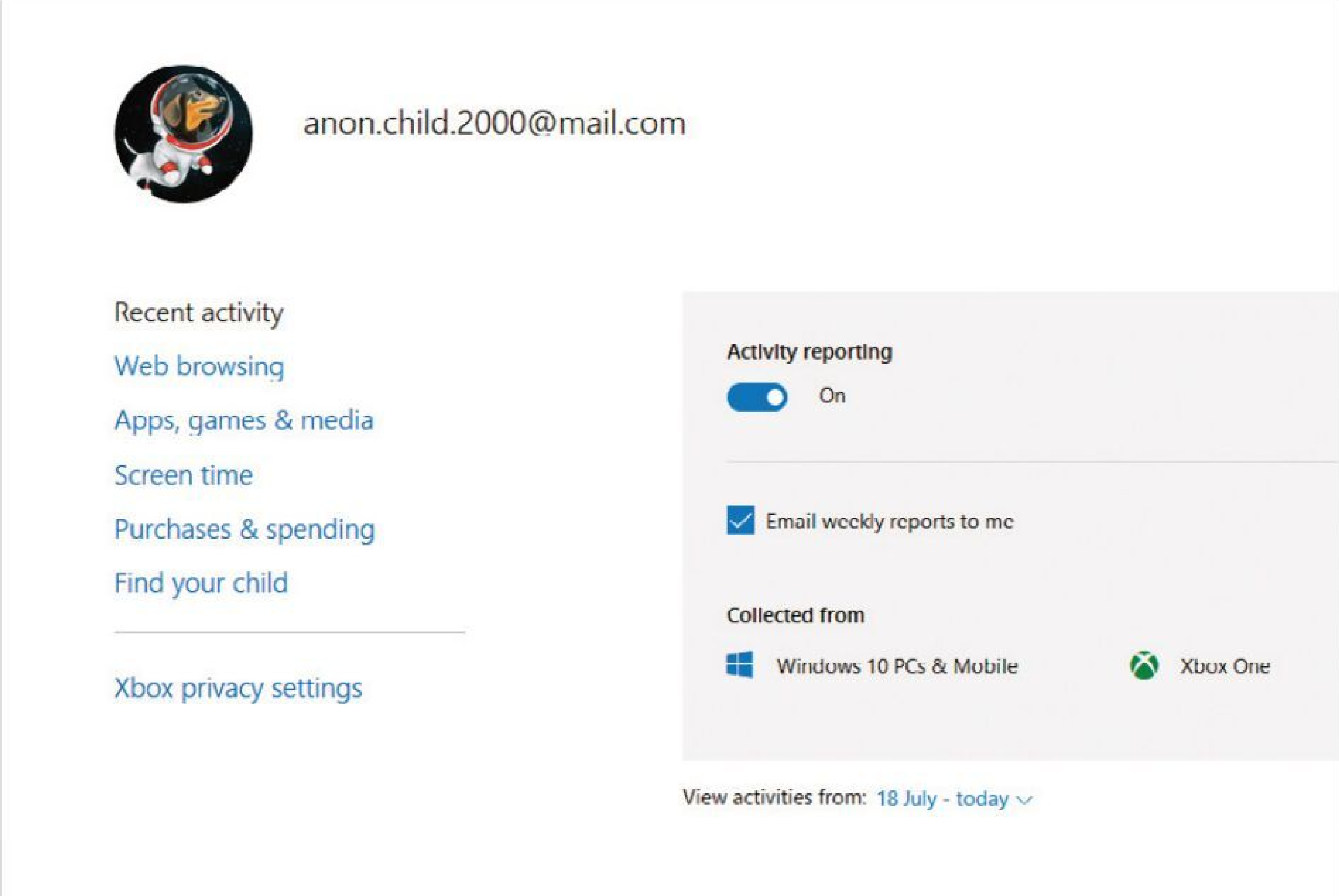
Activity reporting
Off

☑ Email weekly reports to me

Collected from
Windows 10 PCs & Mobile
Xbox One

A window into their digital life
Get recent activity reports on sites visited, apps used, games played and scr

STEP 3 Being a parent or guardian, you can set Activity Reporting for any of your Microsoft child accounts. Click on the Activity reporting slider to the On position; this will instantly block InPrivate browsing within Microsoft Edge and start to collect data on their online activity.


anon.child.2000@mail.com

Recent activity
Web browsing
Apps, games & media
Screen time
Purchases & spending
Find your child
Xbox privacy settings

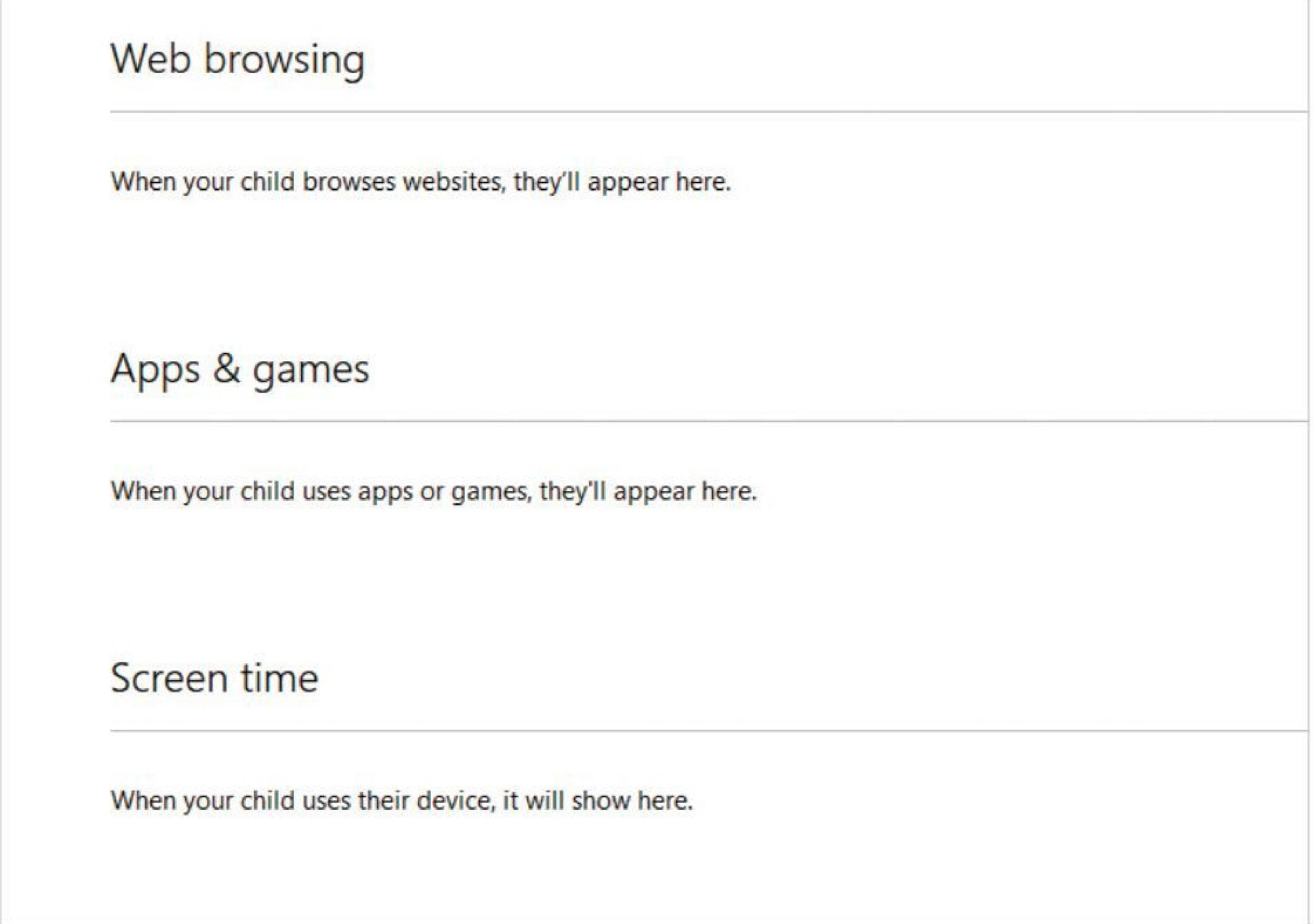
Activity reporting
On

☑ Email weekly reports to me

Collected from
Windows 10 PCs & Mobile
Xbox One

View activities from: 18 July - today

STEP 4 Under the Activity reporting, you can see sections for Web browsing, Apps & games and Screen time. To the right of each title are links to set up web access blocking, game and app blocking and so on. Click on the Turn on blocking link next to Web browsing to begin with.


Web browsing

When your child browses websites, they'll appear here.

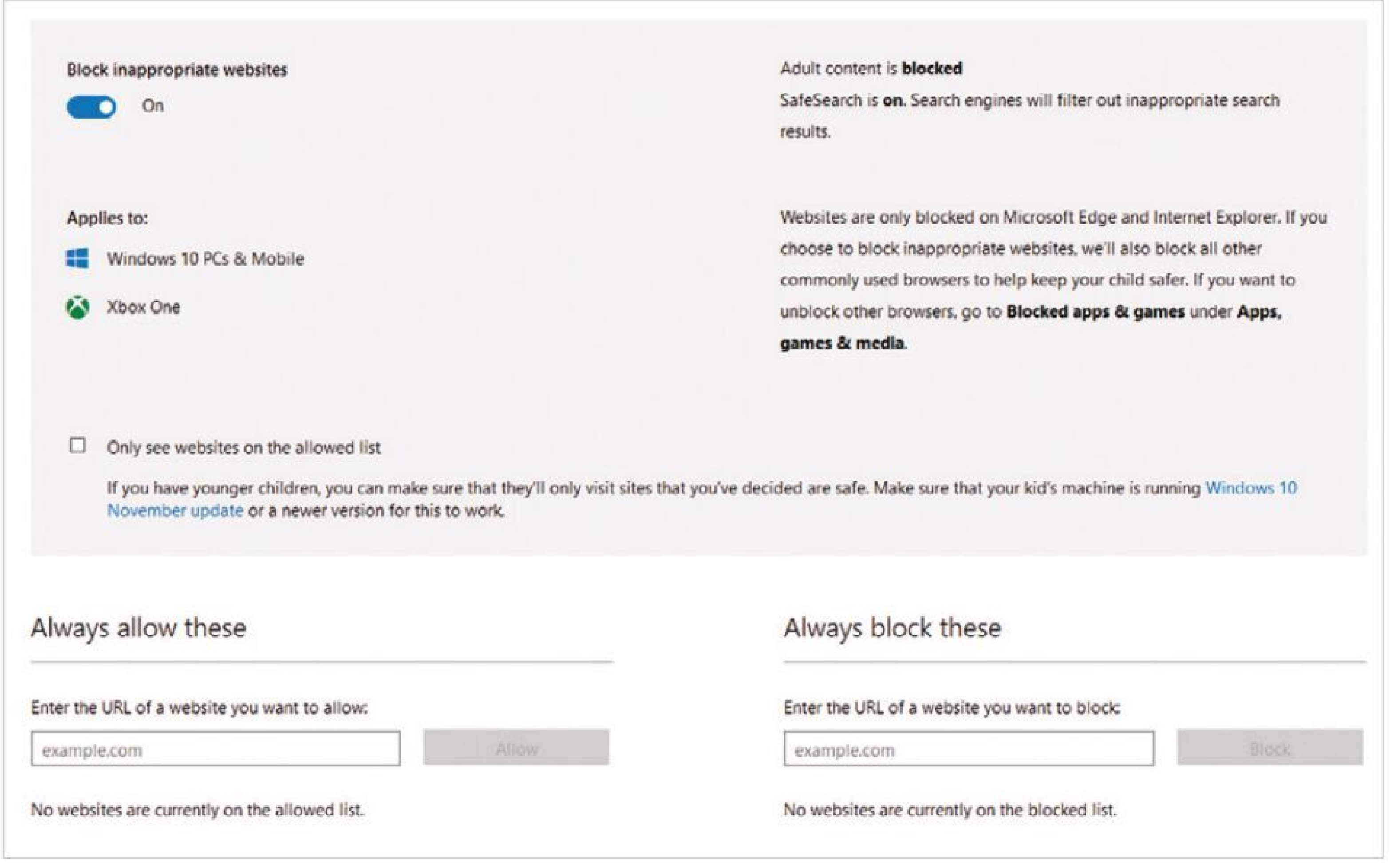
Apps & games

When your child uses apps or games, they'll appear here.

Screen time

When your child uses their device, it will show here.

STEP 5 Providing the child uses Microsoft Edge, you can set Windows 10 to automatically block any inappropriate websites by clicking the slider in the Turn on blocking link to the On position. By default, Microsoft will block all inappropriate sites but you can also specify an allow and block list of sites yourself.



Block inappropriate websites
On

Applies to:
Windows 10 PCs & Mobile
Xbox One

Adult content is **blocked**
SafeSearch is **on**. Search engines will filter out inappropriate search results.

Websites are only blocked on Microsoft Edge and Internet Explorer. If you choose to block inappropriate websites, we'll also block all other commonly used browsers to help keep your child safer. If you want to unblock other browsers, go to **Blocked apps & games** under **Apps, games & media**.

☐ Only see websites on the allowed list

If you have younger children, you can make sure that they'll only visit sites that you've decided are safe. Make sure that your kid's machine is running Windows 10 November update or a newer version for this to work.

Always allow these

Enter the URL of a website you want to allow:
example.com | Allow

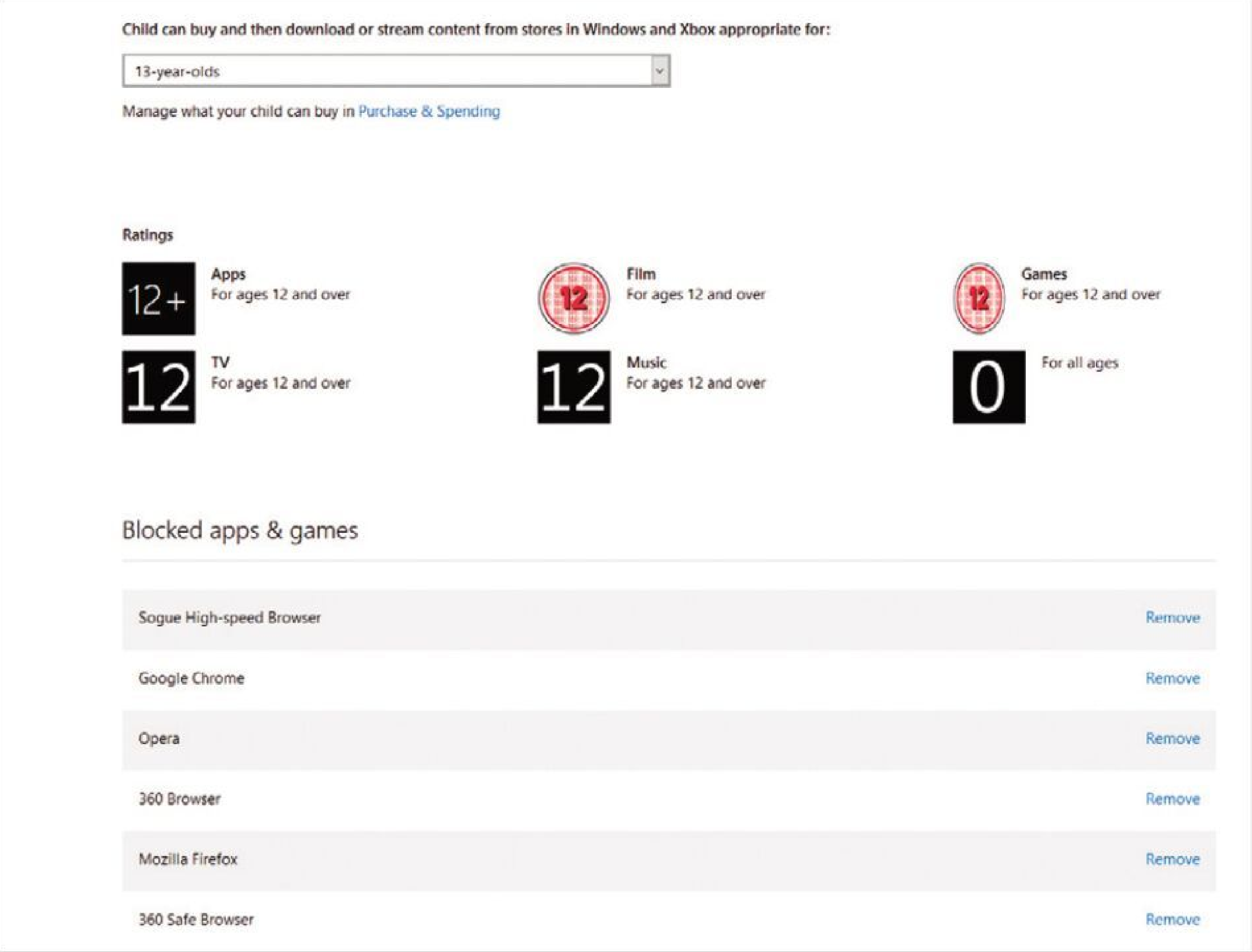
No websites are currently on the allowed list.

Always block these

Enter the URL of a website you want to block:
example.com | Block

No websites are currently on the blocked list.

STEP 6 Click on the back button in your browser to return to the previous page. Now click the Apps & games section and the Changing settings link. In here you can set age-specific restrictions on apps and games, as well as block certain programs from running, such as another browser, forcing them to use MS Edge instead.



Child can buy and then download or stream content from stores in Windows and Xbox appropriate for:
13-year-olds
Manage what your child can buy in Purchase & Spending

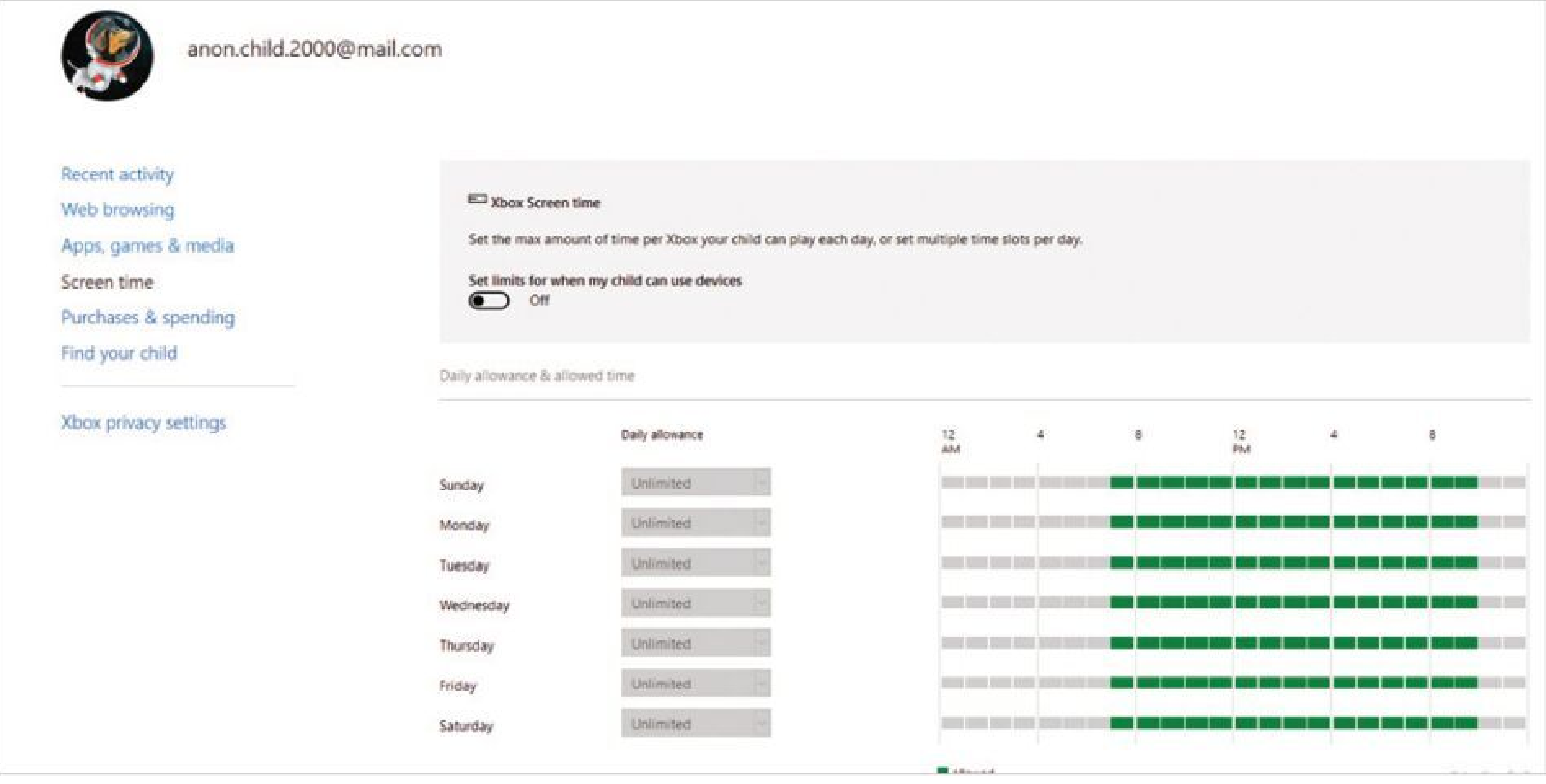
Ratings

12+	**Apps** For ages 12 and over	12	**Film** For ages 12 and over	12	**Games** For ages 12 and over
12	**TV** For ages 12 and over	12	**Music** For ages 12 and over	0	For all ages

Blocked apps & games

Sogue High-speed Browser	Remove
Google Chrome	Remove
Opera	Remove
360 Browser	Remove
Mozilla Firefox	Remove
360 Safe Browser	Remove

STEP 7 Screen time, found on the link to the left under the child's account name, will allow you to set time restrictions for the child. These restrictions will work for Windows 10 computers and devices, as well as Xbox consoles.



anon.child.2000@mail.com

Recent activity
Web browsing
Apps, games & media
Screen time
Purchases & spending
Find your child
Xbox privacy settings

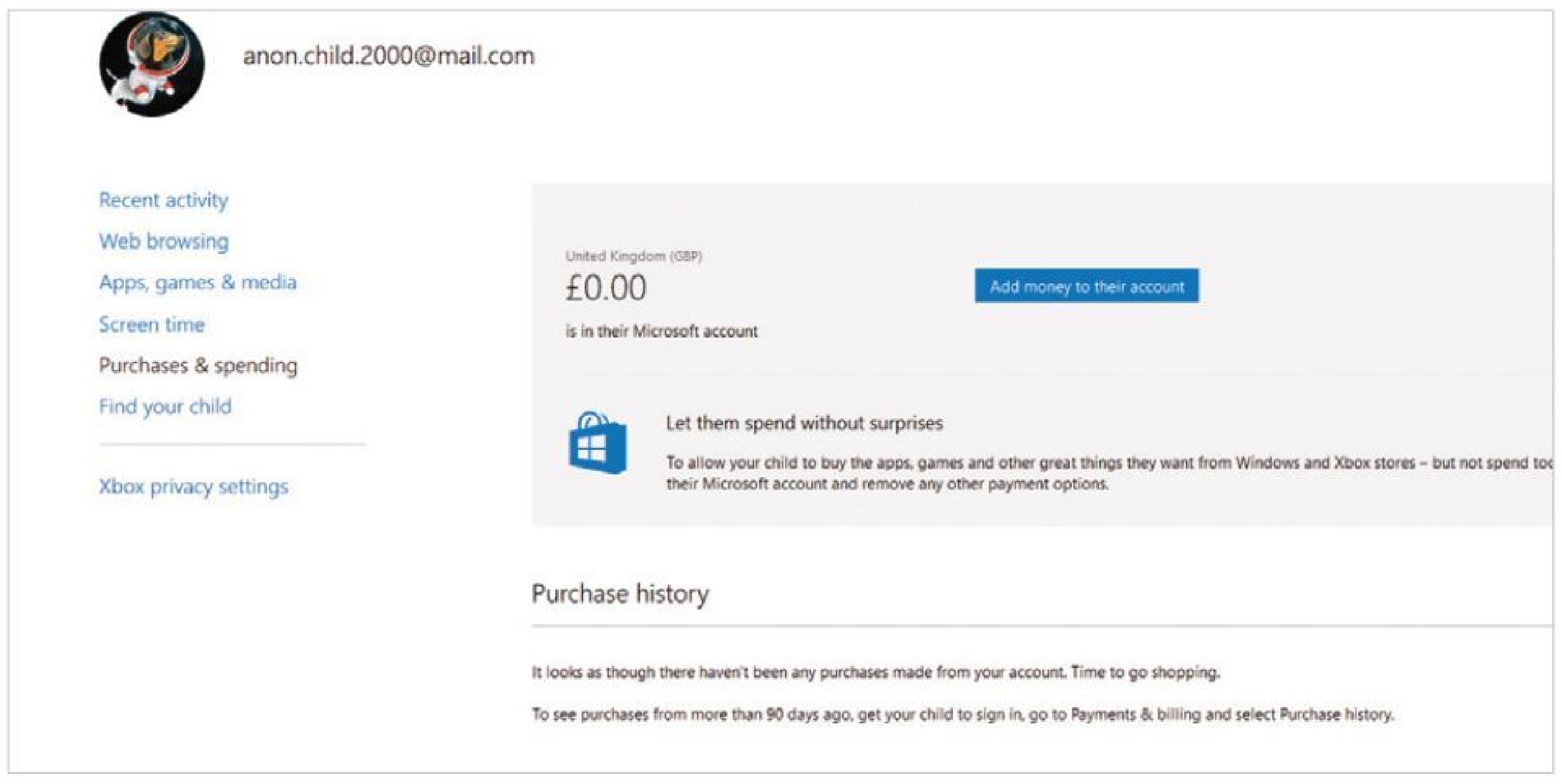
Xbox Screen time
Set the max amount of time per Xbox your child can play each day, or set multiple time slots per day.
Set limits for when my child can use devices
Off

Daily allowance & allowed time

	Daily allowance
Sunday	Unlimited
Monday	Unlimited
Tuesday	Unlimited
Wednesday	Unlimited
Thursday	Unlimited
Friday	Unlimited
Saturday	Unlimited

12 AM
4
8
12 PM
4
8

STEP 8 Purchases & spending is an interesting option and something which we'll be looking at in the next couple of pages. In here, you can specify a spending limit on the child's account as well as view their purchase history.



anon.child.2000@mail.com

Recent activity
Web browsing
Apps, games & media
Screen time
Purchases & spending
Find your child
Xbox privacy settings
Add money to their account

United Kingdom (GBP)
£0.00
is in their Microsoft account

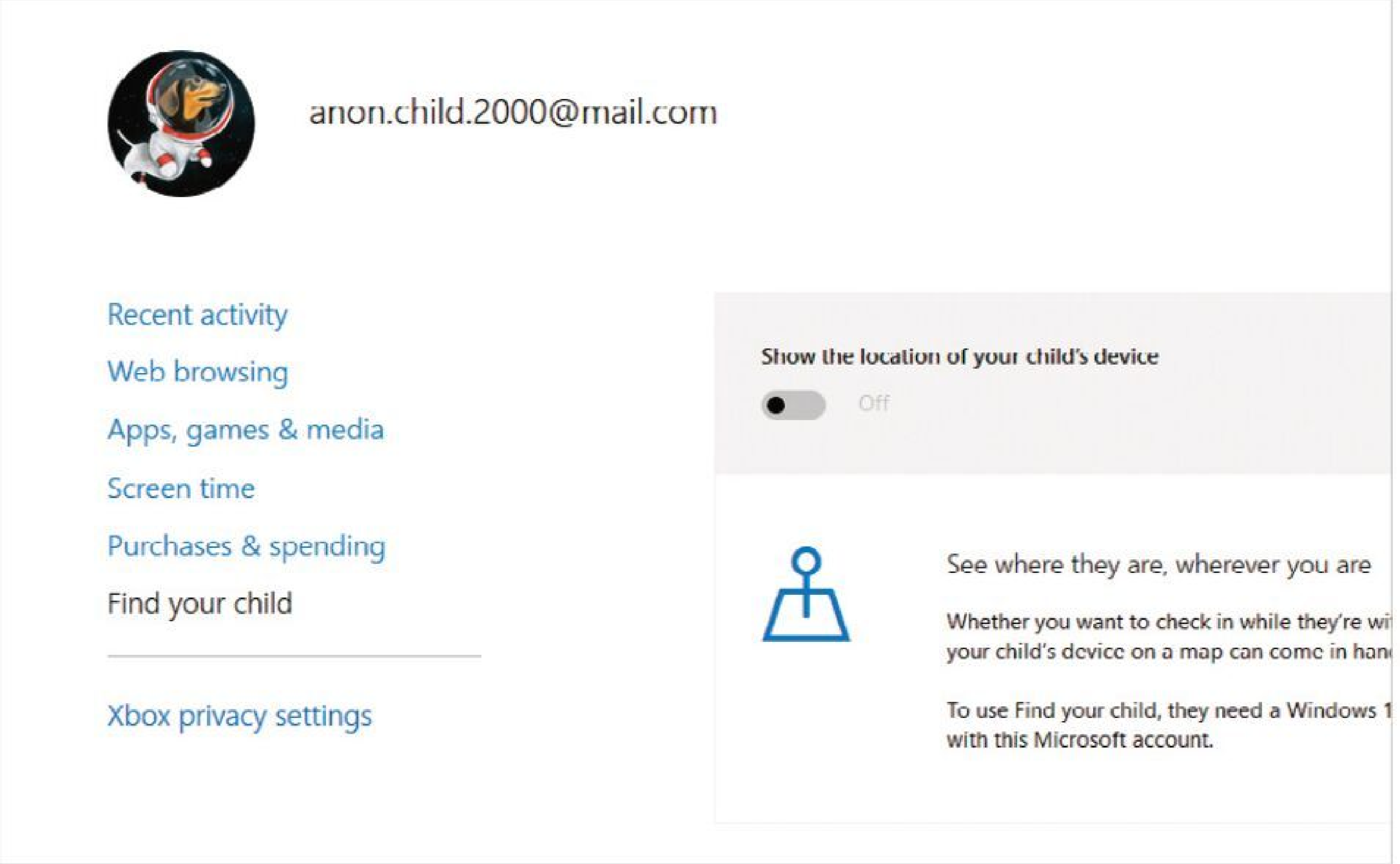
Let them spend without surprises
To allow your child to buy the apps, games and other great things they want from Windows and Xbox stores – but not spend to
their Microsoft account and remove any other payment options.

Purchase history

It looks as though there haven't been any purchases made from your account. Time to go shopping.

To see purchases from more than 90 days ago, get your child to sign in, go to Payments & billing and select Purchase history.

STEP 9 The Find your child setting works only with Windows 10 Mobile devices. With it, you're able to locate your child or rather their device, within just a few metres via a handy map. Useful for if they lose their device or just checking in on where they are.



anon.child.2000@mail.com

Recent activity
Web browsing
Apps, games & media
Screen time
Purchases & spending
Find your child
Xbox privacy settings

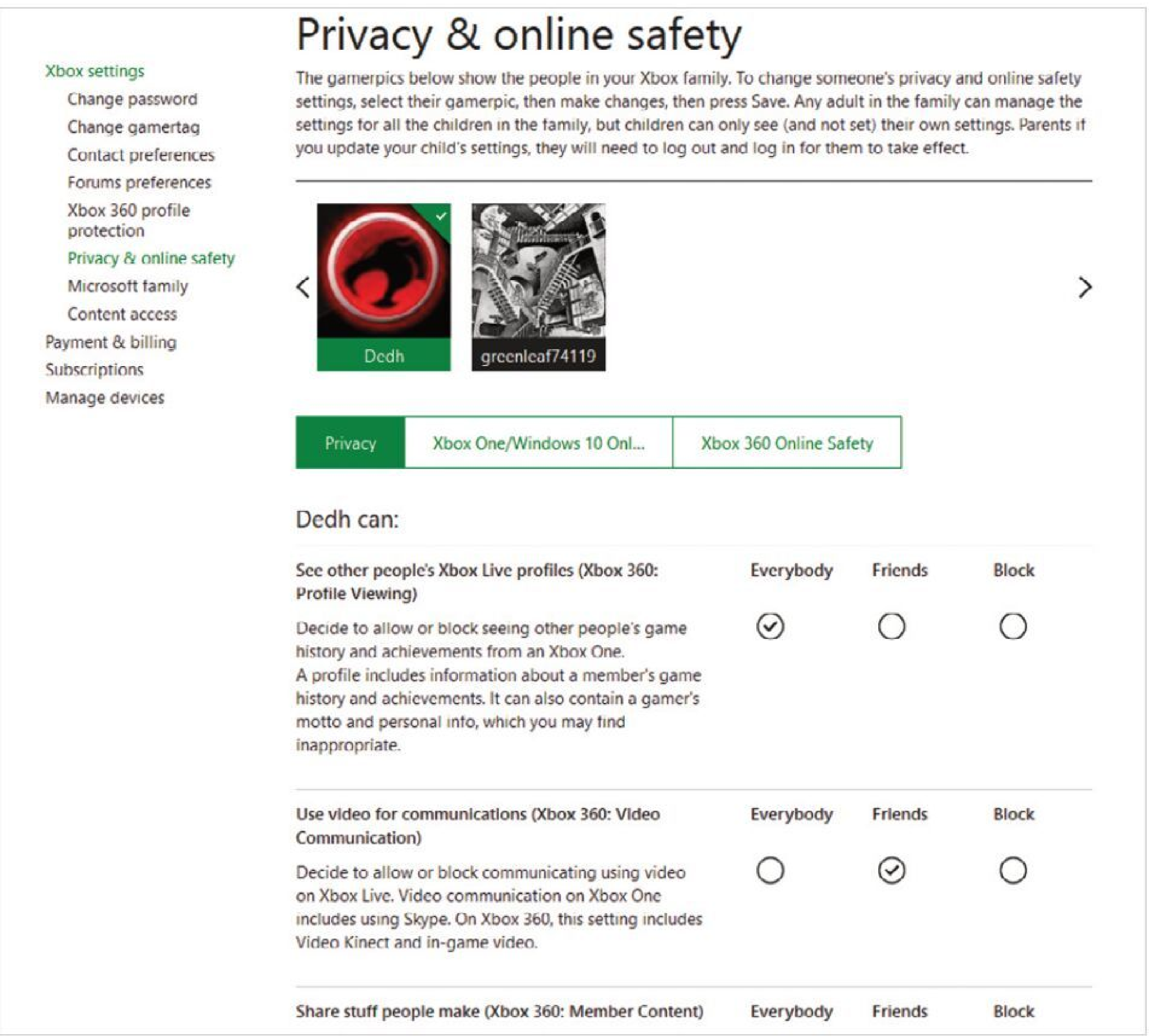
Show the location of your child's device
Off

See where they are, wherever you are

Whether you want to check in while they're wi
your child's device on a map can come in han

To use Find your child, they need a Windows 1
with this Microsoft account.

STEP 10 If you own an Xbox One or Xbox 360, you're also able to set up any Xbox Privacy settings from within the Microsoft Family portal. You can specify video chat, viewing of profiles, sharing and other forms of communications from the console.



Xbox settings
Change password
Change gamertag
Contact preferences
Forums preferences
Xbox 360 profile protection
Privacy & online safety
Microsoft family
Content access
Payment & billing
Subscriptions
Manage devices
Dedh
greenleaf74119
Privacy
Xbox One/Windows 10 Onl...
Xbox 360 Online Safety

Privacy & online safety

The gamerpics below show the people in your Xbox family. To change someone's privacy and online safety settings, select their gamerpic, then make changes, then press Save. Any adult in the family can manage the settings for all the children in the family, but children can only see (and not set) their own settings. Parents if you update your child's settings, they will need to log out and log in for them to take effect.

Dedh can:

	Everybody	Friends	Block
See other people's Xbox Live profiles (Xbox 360: Profile Viewing) Decide to allow or block seeing other people's game history and achievements from an Xbox One. A profile includes information about a member's game history and achievements. It can also contain a gamer's motto and personal info, which you may find inappropriate.	☑	○	○
Use video for communications (Xbox 360: Video Communication) Decide to allow or block communicating using video on Xbox Live. Video communication on Xbox One includes using Skype. On Xbox 360, this setting includes Video Kinect and in-game video.	○	☑	○
Share stuff people make (Xbox 360: Member Content)	Everybody	Friends	Block

Problems with In-app Spending

The Internet is awash with horror stories from parents who have discovered that their child has spent an impressive sum on a game without their consent or knowledge; but, just how much of a problem is this in-app spending issue?

In-app spending is a modern scourge for parents, guardians and even the children and young people themselves. From the point of view of the parent or guardian, we have a child who enjoys playing a game, regardless of whether it's a mobile game, console game or triple-A rated PC game and we're more than happy to allow them to play the game without any restrictions, after all it's just a game, right? However, when those parents then receive the bill from their credit card company, or a call from the bank, that their account is now several hundred or even thousands of pounds lighter, that game has suddenly become the bane of their existence.

From the point of view of the child, they have an incredible and addictive game in front of them. They've put in the hours of game time to achieve a certain level but to get any further in the game, or to beat an end of the level boss or something, they need an extra push. That push can come in the form of more powerful spells, weaponry, armour or whatever else the game requires to boost the player's stats. To get hold of that equipment or bonus content, they need to purchase it from the in-game store. Some of the content costs just a few pounds but it soon lures them into the more expensive extras. Before they realise it, those few pound extras soon add up and the straw that breaks the camel's back is the expensive object that pushes them into the new levels, and causes the parents much angst.

The developers and creators of the game have their point of view too. These developers have spent many hours of coding, testing, re-coding and marketing to help launch their game. It's a painful, exhausting and often expensive process, so the company that launches the game will need to see some good returns if it still wants to continue in business and employing developers, testers and everyone else involved. All these people involved with the game need paying, so if they can top up the business with in-app purchases, added content and such, then why not.

Of course, that doesn't help the parent or guardian who is now looking at their vastly diminished bank account. What there must be is some form of middle ground, where the developers still get paid and the company can keep producing exciting and great games. Here the players get to reach the levels they want and continue playing the game and parents and guardians can safely leave their children to play the game and purchase an upgrade or two, without breaking the bank.

In light of events that hit the headlines, children spending thousands of pounds on purchasing virtual pets, virtual food, more lives etc., the main providers of mobile purchases, such as Apple, Google, Microsoft and so on, started to roll out levels of restrictions to help prevent overspending. These restrictions vary and have improved greatly in recent years; but initially they we're more centred around simple tips and advice for parents rather than the kind of spending restrictions we see today.

Of course, some of the problems also arise when the game in question is clearly a pay-to-win model. It's hardly fair for the young person to enjoy the game when they're continually beaten by those players who can afford to spend the money on extra lives, energy and so on. The pay to play model, on the other hand, requires the purchase of the app before it can even be played. Some experts argue that this is a better model but that's up for debate.

One of the main causes for excessive in-app spending is a child or young person being left alone with the device and game whilst the parent was logged into their own account. The account itself doesn't have any restrictions or password access to get into the online store, after all why would most people continually require password access to their own in-store account; or when the child knows the password and can easily access the store.

The child, left alone, could then go ahead and accept the message from the game that asked 'to continue, buy more apples' (or whatever), which in turn led them directly to the store to place the order in the basket without any kind of confirmation or message stating to check with an adult first.

Most of the time, when these sorts of scenarios occurred, the likes of Apple, Google and so on refunded the parents in question. From there, it became more difficult for a young person to go on an in-game spending spree with their parent's account.

There's a more controlled in-game and in-app spending focus these days but it's still not unheard of for a child to get a little carried away and purchase several hundred on some form of virtual extras for the game. Thankfully, we can combat a sizeable percentage of these cases with a little education and some much-needed tips, which we'll cover on the next couple of pages.

There are two main schools of thought on the Internet regarding the overspending in an app or game by a child. One view is that it's the fault of parents or guardians, letting their child on the game with unrestricted access to their mobile spending platform.

> **Pay to Win**

The other view lies the blame at the feet of the developers and those who have created the app or game. Both have their valid points, and there's no right or wrong, but perhaps the blame lies equally with each.

Tips on How to Stop In-app Overspending

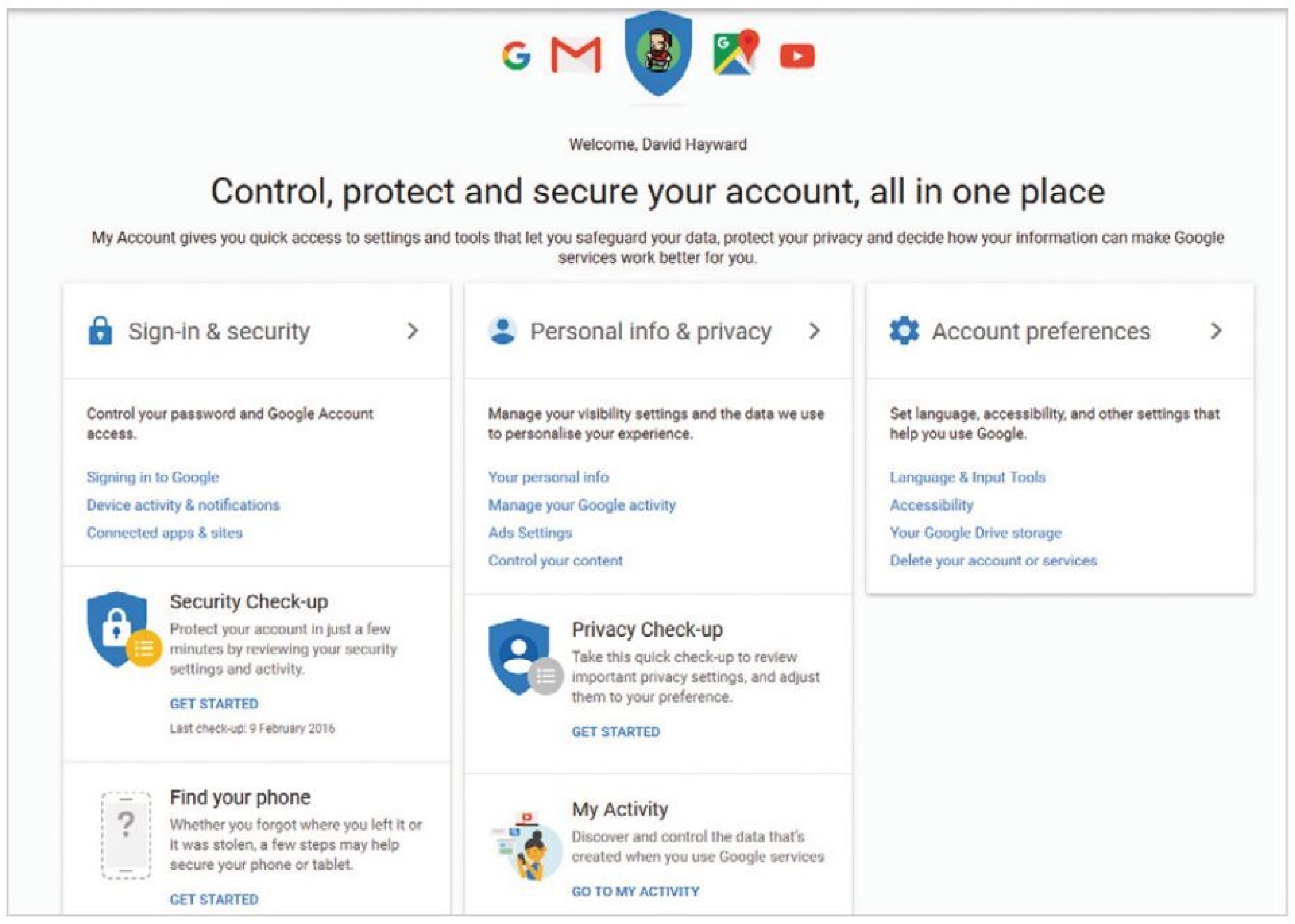
In-app overspending, as we've seen, is a concern for parents and guardians whenever their children use a phone, tablet, console or computer. However, there is a happy middle ground, where the kids can still enjoy their game and the parents needn't worry about in-app purchases.

10 Tips to Stop In-app Purchases

There's nothing wrong with spending money on a game, either to buy it in the first place or just to upgrade a part of it. What's needed though, is a little thought to combat overspending.

TIP 1 The main tip, and one that all child experts agree on, is simply don't leave your child alone with a device, console or computer whilst playing the game. Naturally it depends on the age of the child but essentially it's recommended never to leave a younger child alone, as that's when rogue spending can occur.

TIP 2 Set up their own account: using a child's account will dramatically cut down on any in-app overspending. Generally speaking, most children won't have access to a bank card to enter into the in-game shop or have access to the family bank details.



Welcome, David Hayward

Control, protect and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy and decide how your information can make Google services work better for you.

Sign-in & security

Control your password and Google Account access.

Signing in to Google
Device activity & notifications
Connected apps & sites

Security Check-up

Protect your account in just a few minutes by reviewing your security settings and activity.

GET STARTED

Last check-up: 9 February 2016

Find your phone

Whether you forgot where you left it or it was stolen, a few steps may help secure your phone or tablet.

GET STARTED

Personal info & privacy

Manage your visibility settings and the data we use to personalise your experience.

Your personal info
Manage your Google activity
Ads Settings
Control your content

Privacy Check-up

Take this quick check-up to review important privacy settings, and adjust them to your preference.

GET STARTED

My Activity

Discover and control the data that's created when you use Google services

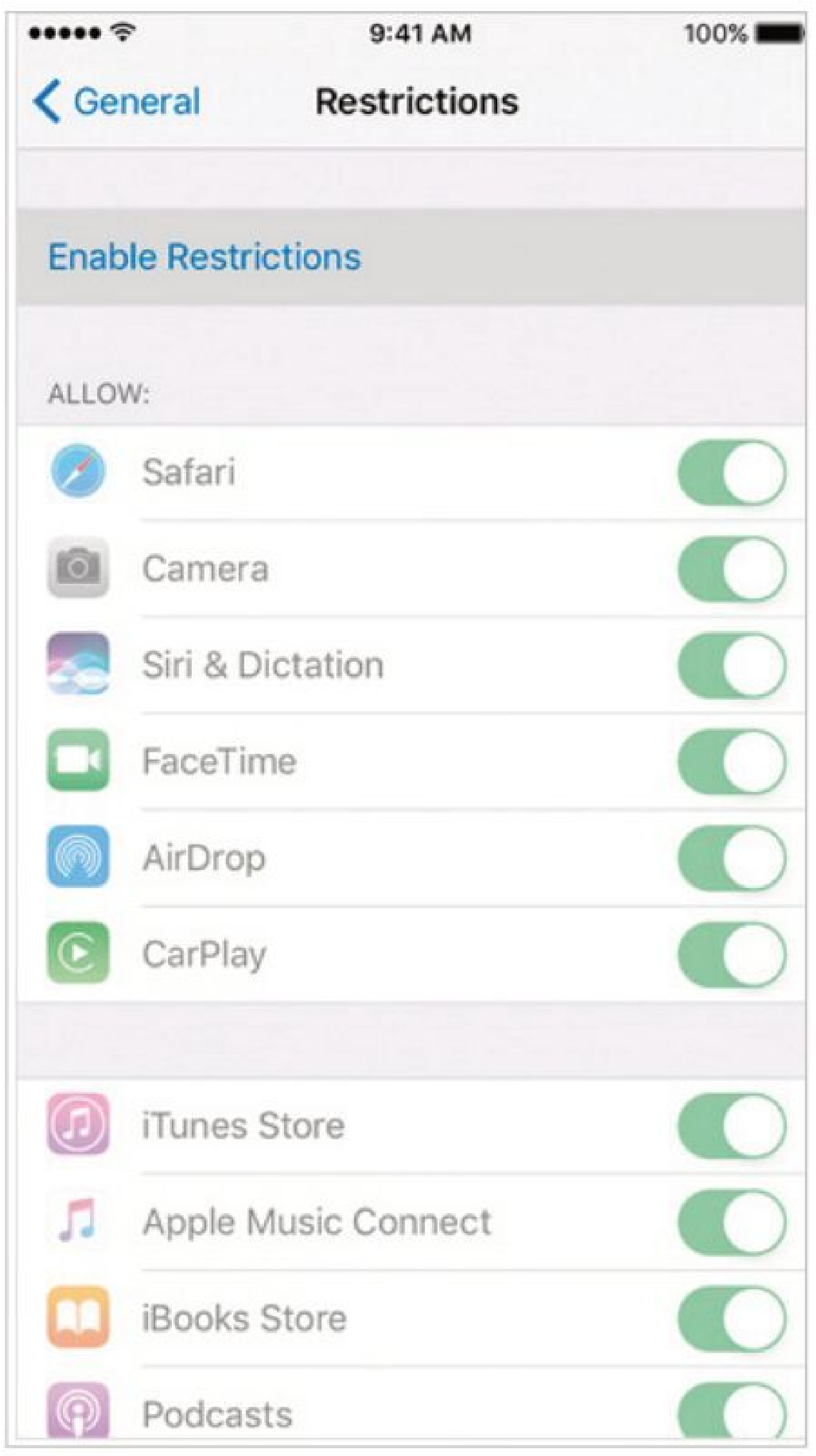
GO TO MY ACTIVITY

Account preferences

Set language, accessibility, and other settings that help you use Google.

Language & Input Tools
Accessibility
Your Google Drive storage
Delete your account or services

TIP 3 If you're using an iOS device, go to Settings > General > Restrictions and tap to enable the Restrictions. You can now create a passcode to lock out access to the iTunes Store, Safari and other Apple online portals, as well as other Apple apps.



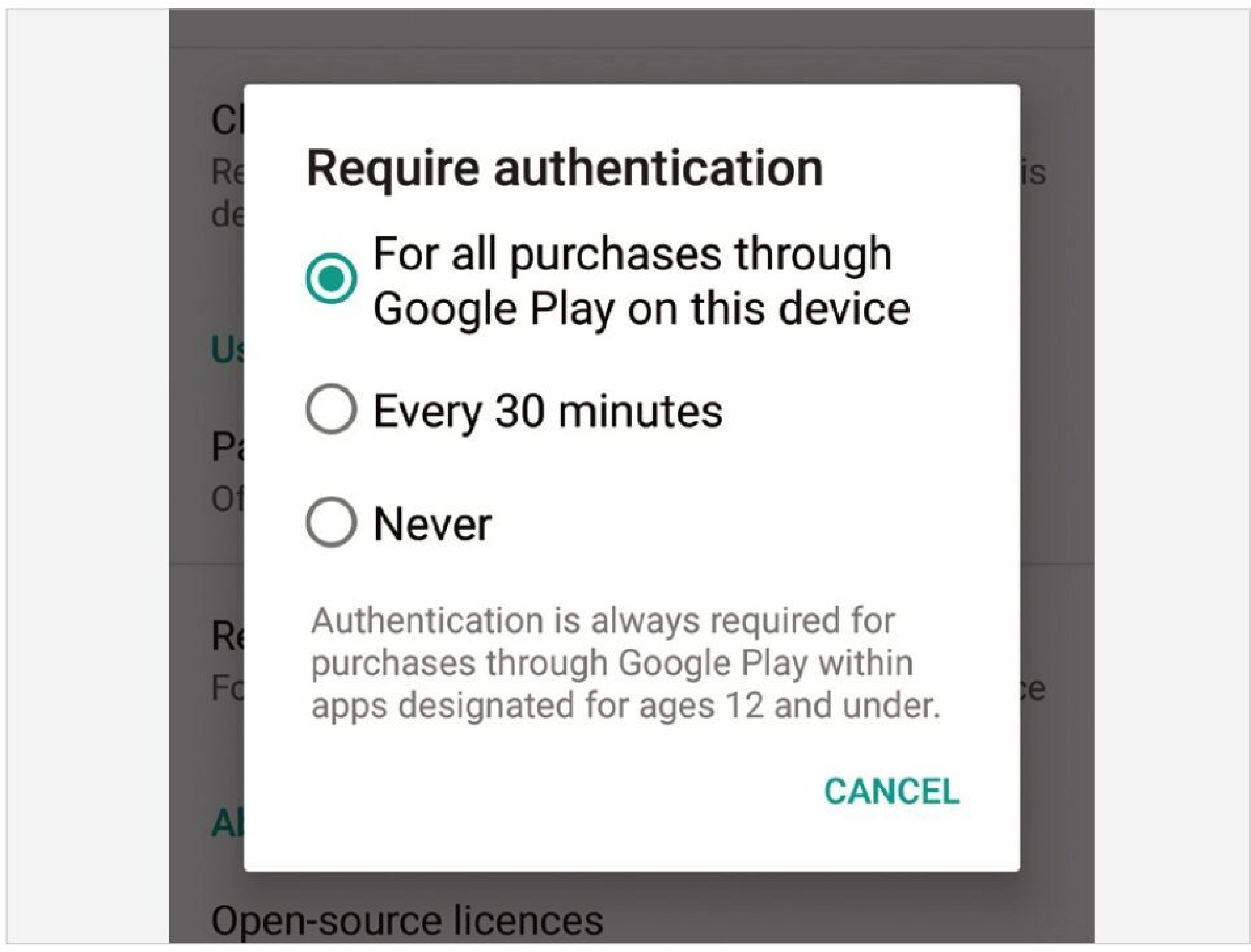
Restrictions

Enable Restrictions

ALLOW:

Safari
Camera
Siri & Dictation
FaceTime
AirDrop
CarPlay
iTunes Store
Apple Music Connect
iBooks Store
Podcasts

TIP 4 For Google devices, it's best to either never enter your banking details into Google Play or swipe in from the left whilst in the Play Store, choose Settings and tap the Require Authentication for Purchases option.

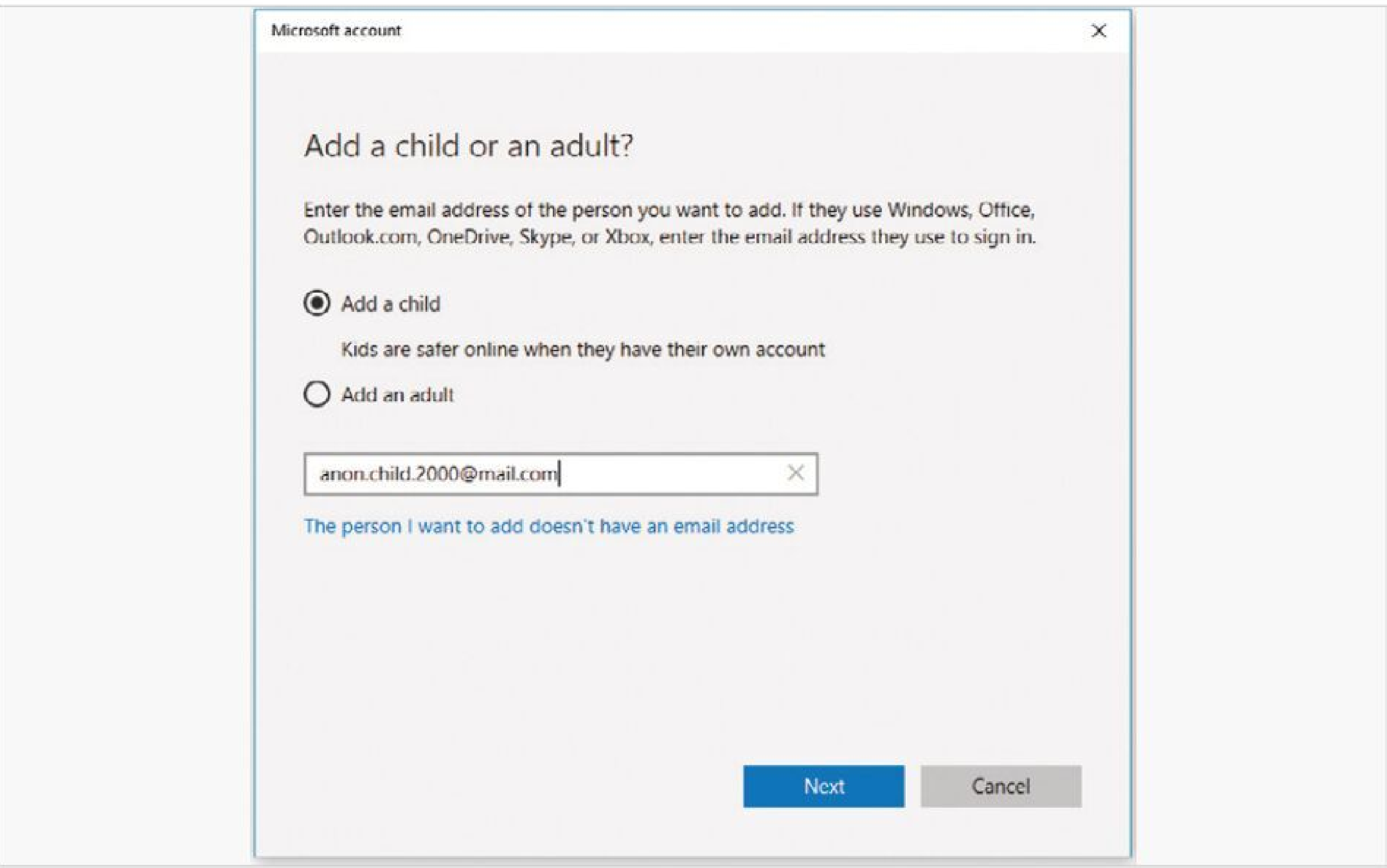


Require authentication

● For all purchases through Google Play on this device
○ Every 30 minutes
○ Never

Authentication is always required for purchases through Google Play within apps designated for ages 12 and under.

TIP 5 For Microsoft accounts, use the steps from our previous pages to create a child's account on your Windows 10 device; then use the Microsoft Family portal to restrict access to apps and spending.


Microsoft account

Add a child or an adult?

Enter the email address of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email address they use to sign in.

● Add a child

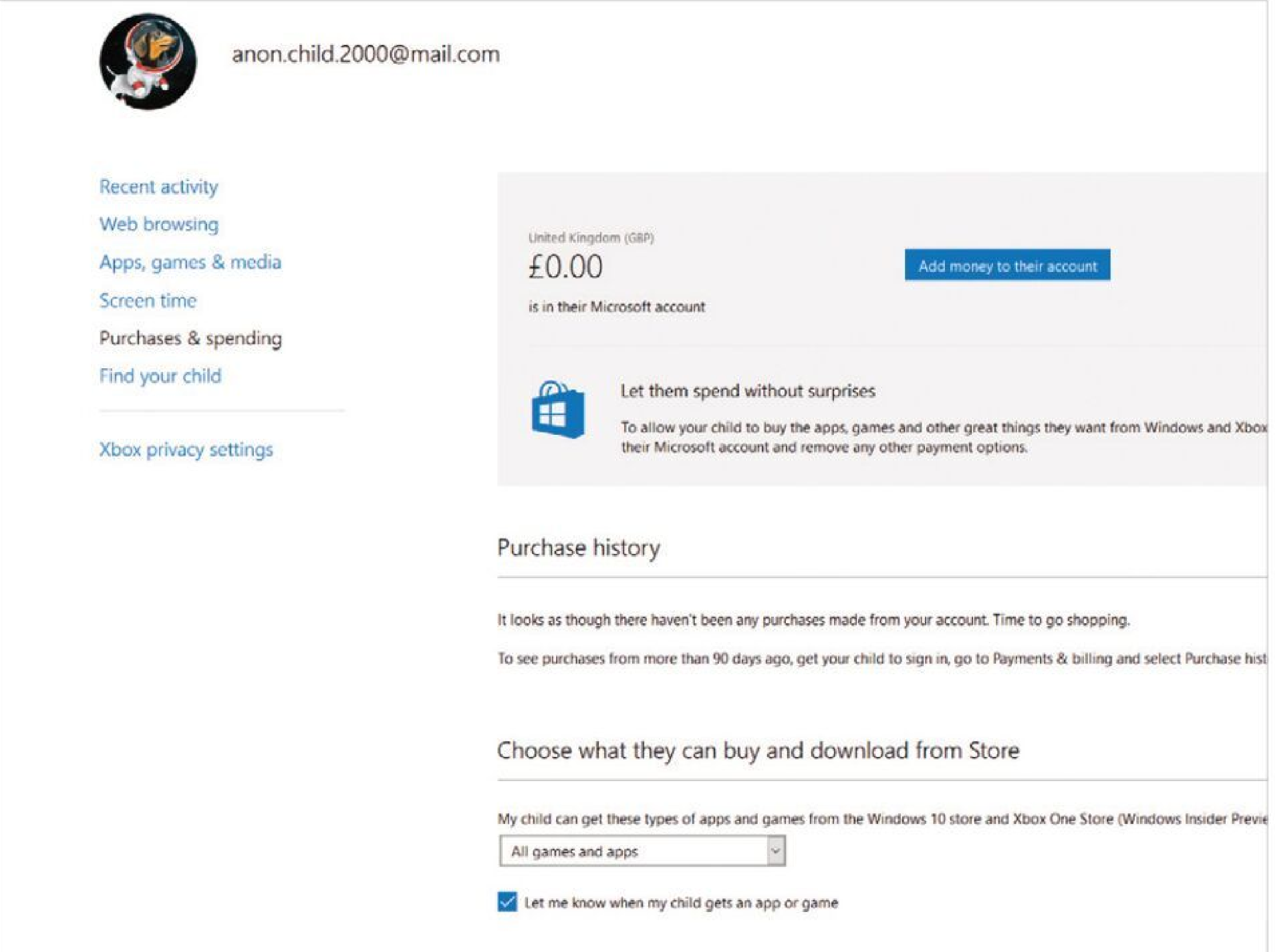
Kids are safer online when they have their own account

○ Add an adult

anon.child.2000@mail.com

The person I want to add doesn't have an email address

TIP 6 There's nothing wrong with spending money on a game, so why not consider setting up a limited amount of money on a Microsoft account. The child then has to then manage their own budget on in-app spending.


anon.child.2000@mail.com

United Kingdom (GBP)
£0.00
is in their Microsoft account

Let them spend without surprises

To allow your child to buy the apps, games and other great things they want from Windows and Xbox their Microsoft account and remove any other payment options.

Purchase history

It looks as though there haven't been any purchases made from your account. Time to go shopping.

To see purchases from more than 90 days ago, get your child to sign in, go to Payments & billing and select Purchase hist

Choose what they can buy and download from Store

My child can get these types of apps and games from the Windows 10 store and Xbox One Store (Windows Insider Previe

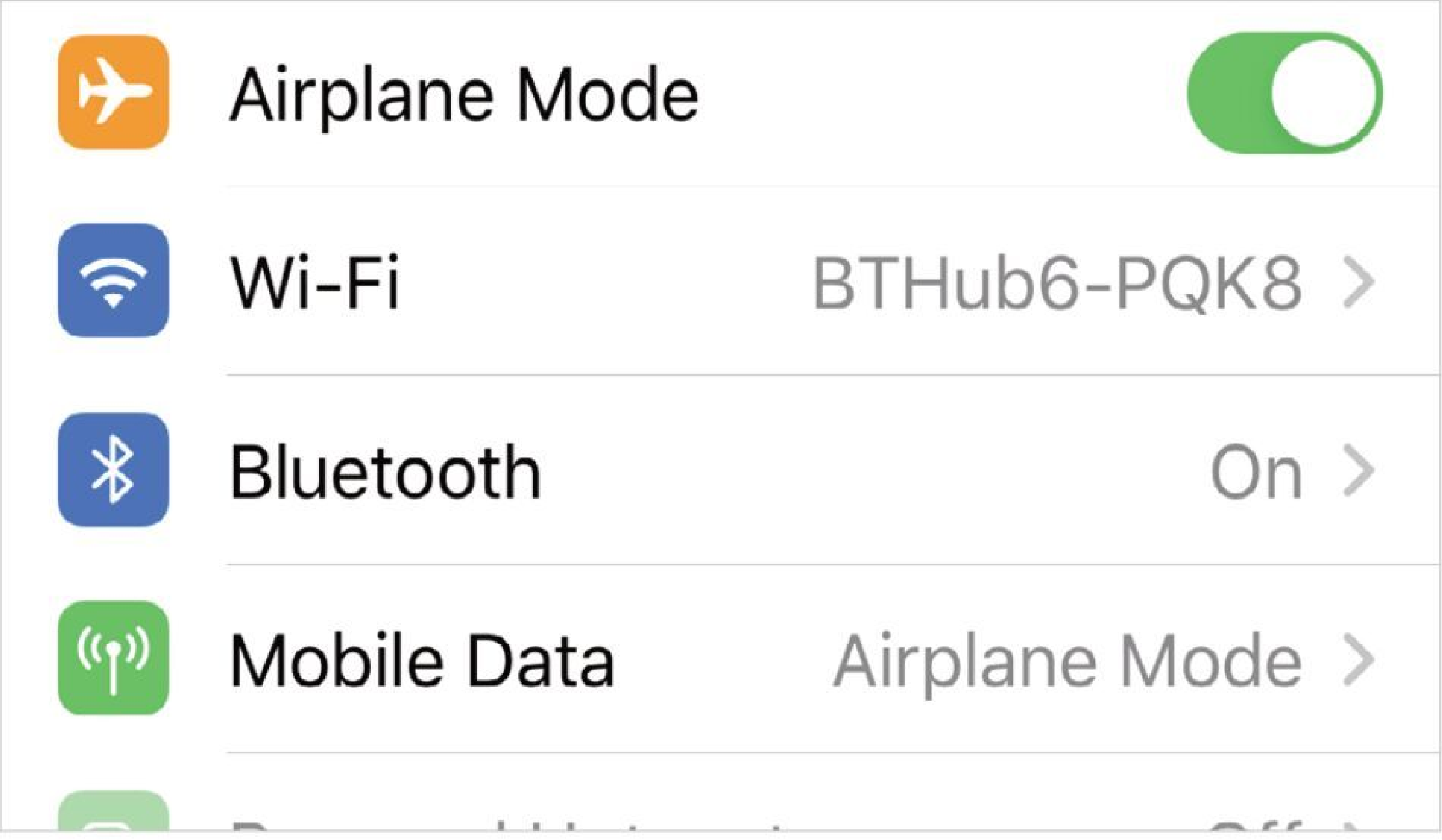
All games and apps

☑ Let me know when my child gets an app or game

TIP 7 Similarly, consider using a gift card for iTunes or Google Play to allow any in-app spending. This way it's a more controlled purchasing environment and since the child is happy with the bonus app-extras, you're happy with the spending and the developer still gets paid. Everyone is happy with the outcome.

£10
Google play
MUSICMOVIESBOOKSAPPS&MORE
£25
£50

TIP 8 Enabling Airplane mode whilst the child is playing on the device stops any access to online services and thus the in-app or in-game stores. It's not ideal, and it can easily be deactivated, but for younger children it's a valid option.


Airplane Mode

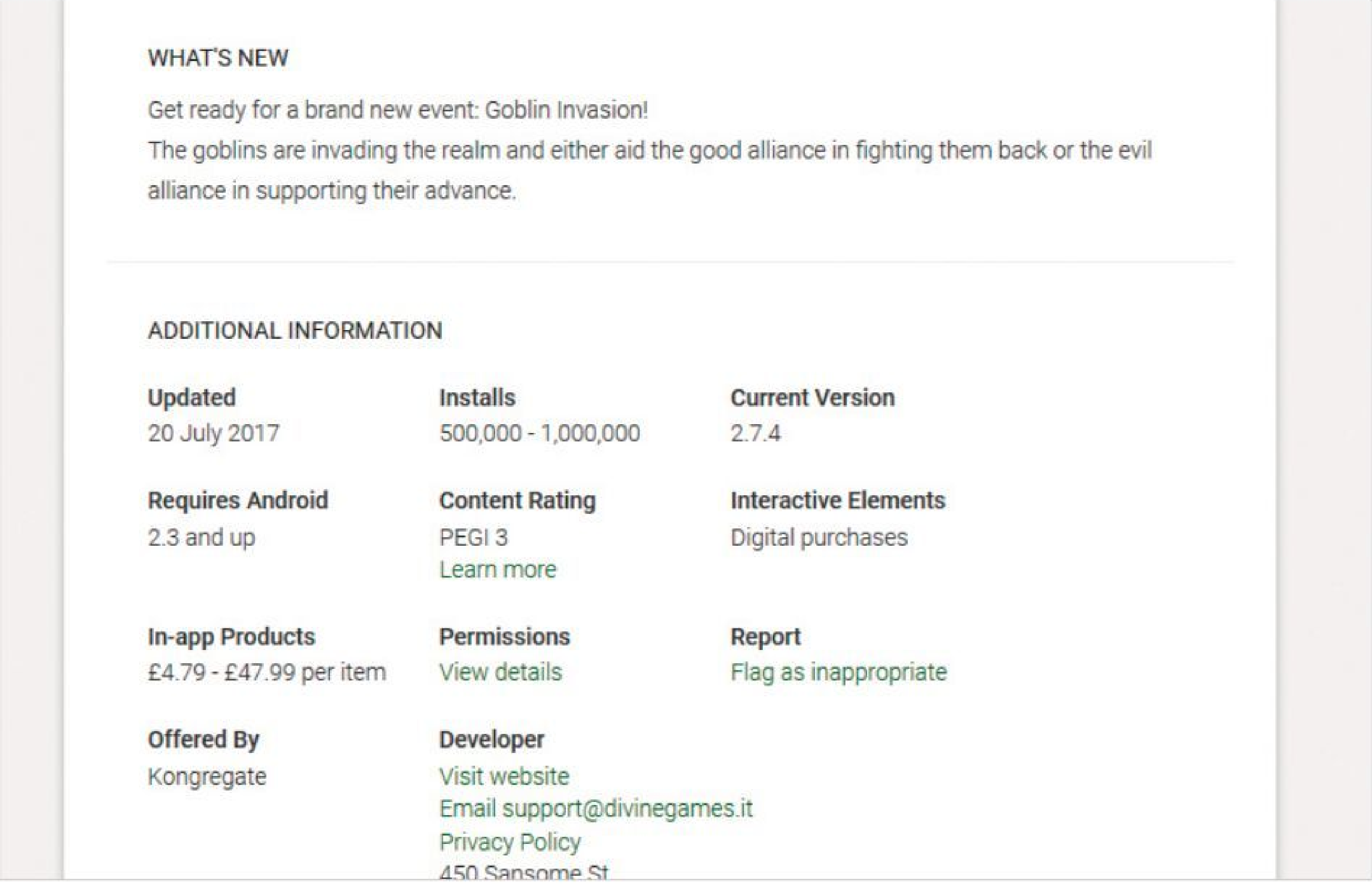
Wi-Fi BTHub6-PQK8

Bluetooth On

Mobile Data Airplane Mode

TIP 9 Talking to your children and taking the time to explain how in-app purchases work, and how bad it can be if they overspend, is a highly recommended option. Child experts state that the best policy to prevent overspending in apps and games is a little education.

TIP 10 Before your child downloads and installs a game or app, take a few moments to look through the app's information to see what, if any, in-app products are on offer. This section will usually inform you of how much money the in-app extras cost and you can then judge whether to allow the install or not.


WHAT'S NEW

Get ready for a brand new event: Goblin Invasion!
The goblins are invading the realm and either aid the good alliance in fighting them back or the evil alliance in supporting their advance.

ADDITIONAL INFORMATION

Updated
20 July 2017

Installs
500,000 - 1,000,000

Current Version
2.7.4

Requires Android
2.3 and up

Content Rating
PEGI 3
Learn more

Interactive Elements
Digital purchases

In-app Products
£4.79 - £47.99 per item

Permissions
View details

Report
Flag as inappropriate

Offered By
Kongregate

Developer
Visit website
Email support@divinegames.it
Privacy Policy
450 Sansome St

Online Child Safety at School

Whilst you're doing everything you can at home to ensure your child is safe when online, what happens when they're out of the protection of your home network? Schools are up against as much, if not more, online safety issues as parents.

How does your child's school provide online safety? What tools and procedures do they use? What government backed schemes are available for them?

> “Safer Schooling”

What's their policy on cyber bullying and what's the process should anything inappropriate ever make its way into the school's network?

Most of those questions are dependent on the school itself and what policies it's created in collaboration with the council, local government, parents, teachers and governing body. In the UK, the UKCCIS (UK Council for Child Internet Safety) has drawn up and developed a guide for school governors to follow, to help governing boards support their school leaders in keeping children safe online. It's an interesting six-page document and further reading can be found with the accompanying Sexting in Schools and Colleges 50-page guidance document. You can find both at *https://www.gov.uk/government/groups/uk-council-for-child-Internet-safety-ukccis*.

From 22 December 2015, the Department for Education put in place strengthened measures to help protect children from harm online, which included cyber bullying, access to pornography and the risks involved with radicalisation. These measures enforced schools to improve or implement better filters and monitoring systems, guides on social media and good practise and the teaching of online threats and the issues surrounding it.

This safeguarding of students through education is one of the best forms of introducing a heightened level of Internet safety amongst young people. Parents and guardians can rant and rave about Internet safety until they are blue in the face but when it comes as part of a lesson in the school, the message is considered to be delivered with a more meaningful impact. In classes, students are taught what Internet use is acceptable, and what isn't and given clear objectives for Internet use. The school is also capable and often required to consult with outside child protection agencies, bringing in experts to help further the student's understanding of the dangers and risks of the Internet, social media and all forms of digital behaviour.

Beyond the classroom talks and conversations, schools employ an assortment of advanced monitoring tools and filters. The school's expert IT staff will already use a range of network level security features found only in the server versions of Windows, or Linux. These features will restrict the students' activities, whilst still offering them access to much needed resources both internally and externally on the Internet. If your child is new to the school, take a moment to ask if you can speak to the head of the school's IT or IT manager and ask them what they use and do to set limits and restrictions on local and Internet resources. Most of the techniques used are quite fascinating, even from a non-technical point of view, and often can be applied to a lesser, but just as effective, degree on the home network.

In addition to protection on the network level, the IT team will also implement a range of site-level Net Nanny-like programs. They may only use a single program, installed on a server to manage each workstation or they may use several programs to manage each student's account; monitoring sites visited and providing blocks for sites that are deemed inappropriate. Another element to consider with a schools' IT is the use of its available bandwidth. With hundreds, often thousands, of devices and computers attached to the school network it can at times become a little slow, as there's limited bandwidth. A school's IT team therefore must also decide whether or not to block access to sites that will cause a strain on the bandwidth, such as online game sites or media streaming. Whilst the students may be blocked from such sites, the teachers are usually unrestricted, for teaching purposes.

These filters, blocked sites and bandwidth monitoring techniques all add up to make an effective protection net around the school's IT infrastructure. It's important to understand, from a parent's point of view, the amount of work needed to achieve such a high degree of online safety and that it can become quite expensive once you factor in licensed software. Where you might have purchased a child filtering product, and employed some of the security techniques we've used in this book, a school IT system needs to do all that times a thousand-plus for each student, computer and device.

Nevertheless, a school's online safety requirements are exceptionally more advanced than you have at home. With this in mind, your child is less likely to experience any online risks when at school than at home. However, it's always best to take the time to make an appointment with the school to ask what they're doing to ensure online safety.

Where to Find Help with Online Child Safety

The tips and features throughout this book will help you build a better understanding of security and online safety, with special reference to online child safety. If you want to know more though, or you have some pressing questions that need answering, here are some places to check out.

Help is at Hand

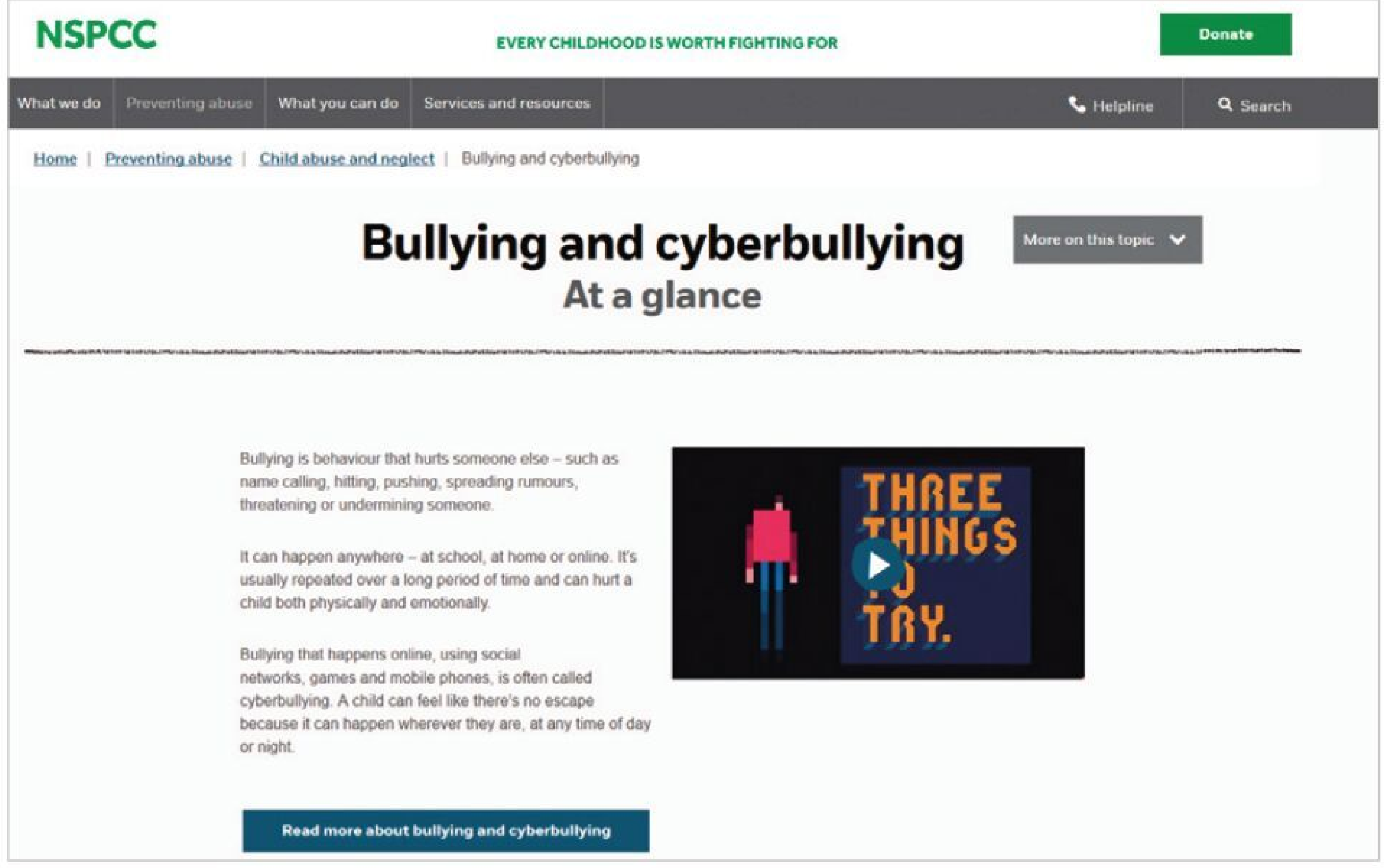
For more information, expert advice from child care professionals and more tips on how to protect your child when online, here are ten sites to bookmark and consider.

TIP 1 If you'd rather contact a professional child care expert, person to person, then consider contacting your local doctor's surgery and asking for a list of contact details of the child counsellors in the area. Most surgeries will have all the relevant information to hand for you.

Doctors
Surgery

TIP 2 Your child's teachers and school welfare officers will have an excellent understanding of how to help keep your child safe when online. They can answer your questions or at least help point you in the right direction.

TIP 3 Regardless of where you are in the world, the UK's NSPCC website contains invaluable information regarding child safety, especially online child safety. You can find the main site at **https://www.nspcc.org.uk/**, with access to services and resources.


NSPCC
EVERY CHILDHOOD IS WORTH FIGHTING FOR
Donate
What we do
Preventing abuse
What you can do
Services and resources
Helpline
Search
Home | Preventing abuse | Child abuse and neglect | Bullying and cyberbullying
More on this topic
THREE THINGS TO TRY.
Read more about bullying and cyberbullying

Bullying and cyberbullying

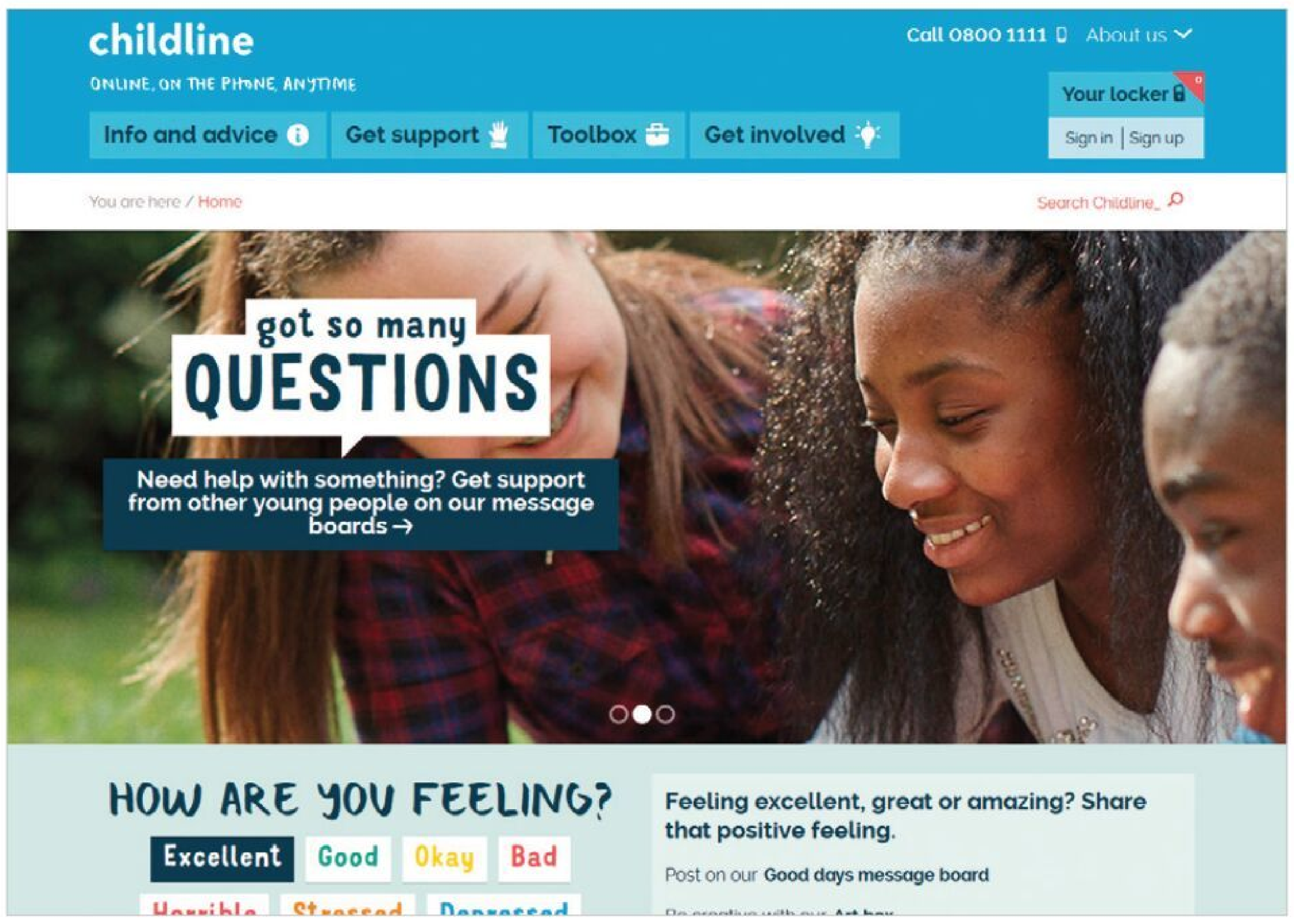
At a glance

Bullying is behaviour that hurts someone else – such as name calling, hitting, pushing, spreading rumours, threatening or undermining someone.

It can happen anywhere – at school, at home or online. It's usually repeated over a long period of time and can hurt a child both physically and emotionally.

Bullying that happens online, using social networks, games and mobile phones, is often called cyberbullying. A child can feel like there's no escape because it can happen wherever they are, at any time of day or night.

TIP 4 In addition to the NSPCC, the UK's Childline is also an exceptional resource that contains a wealth of information and support for families, parents, guardians and children. There's a superb online safety section too. You can find Childline at **https://www.childline.org.uk/**.

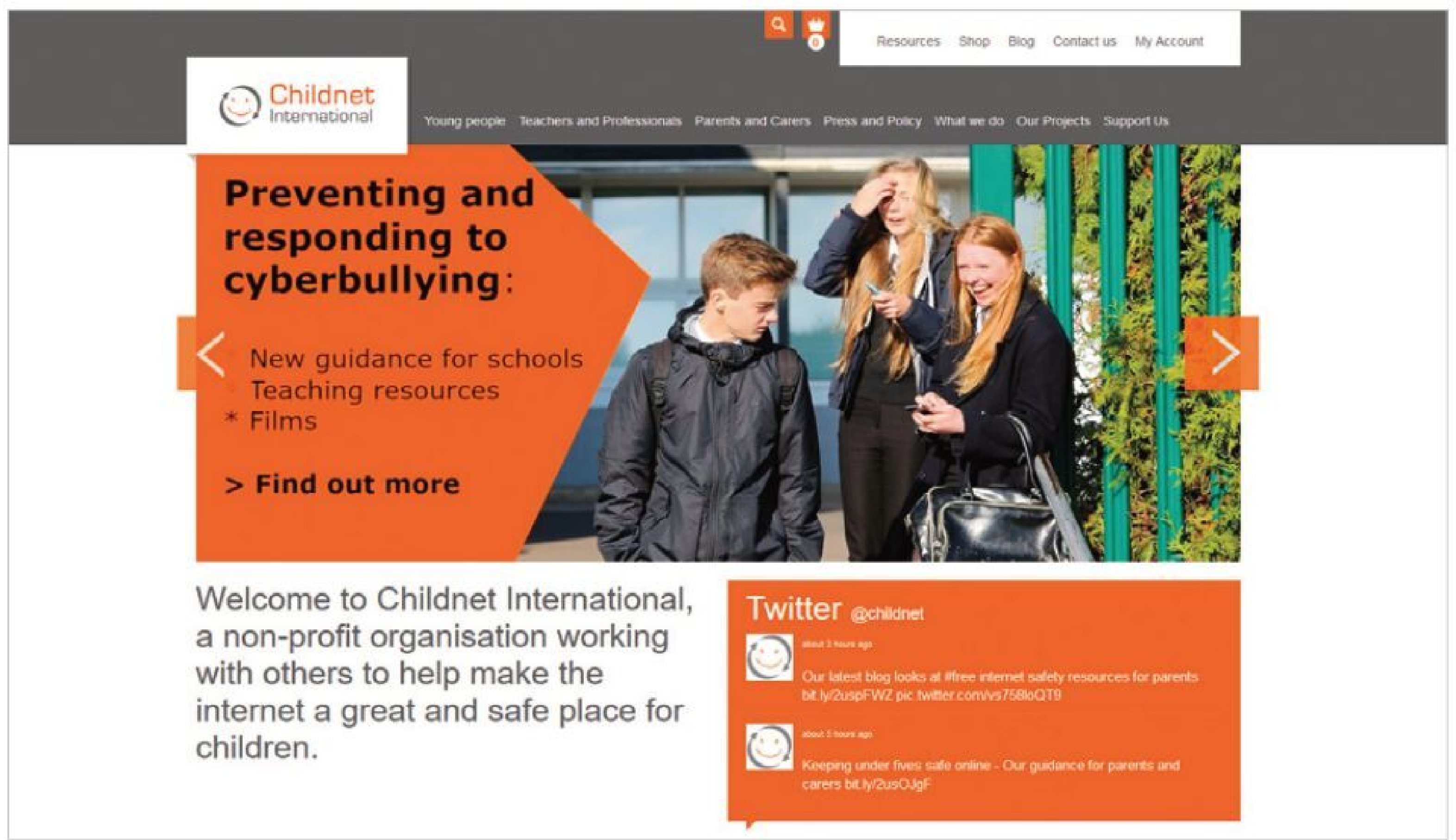

childline
ONLINE, ON THE PHONE, ANYTIME
Call 0800 1111
About us
Your locker
Sign in | Sign up
Info and advice
Get support
Toolbox
Get involved
You are here / Home
Search Childline
got so many QUESTIONS
HOW ARE YOU FEELING?
Excellent
Good
Okay
Bad

Need help with something? Get support from other young people on our message boards →

Feeling excellent, great or amazing? Share that positive feeling.

Post on our **Good days message board**

TIP 5 Childnet International is a site dedicated to young people, children, teachers and professionals, parents and carers. There's a ton of resources and support available through the site and plenty of advice about online child safety. Find it at **http://www.childnet.com/**.


Resources
Shop
Blog
Contact us
My Account
Childnet International
Young people
Teachers and Professionals
Parents and Carers
Press and Policy
What we do
Our Projects
Support Us
Twitter @childnet

Preventing and responding to cyberbullying:

- New guidance for schools
- Teaching resources
- Films

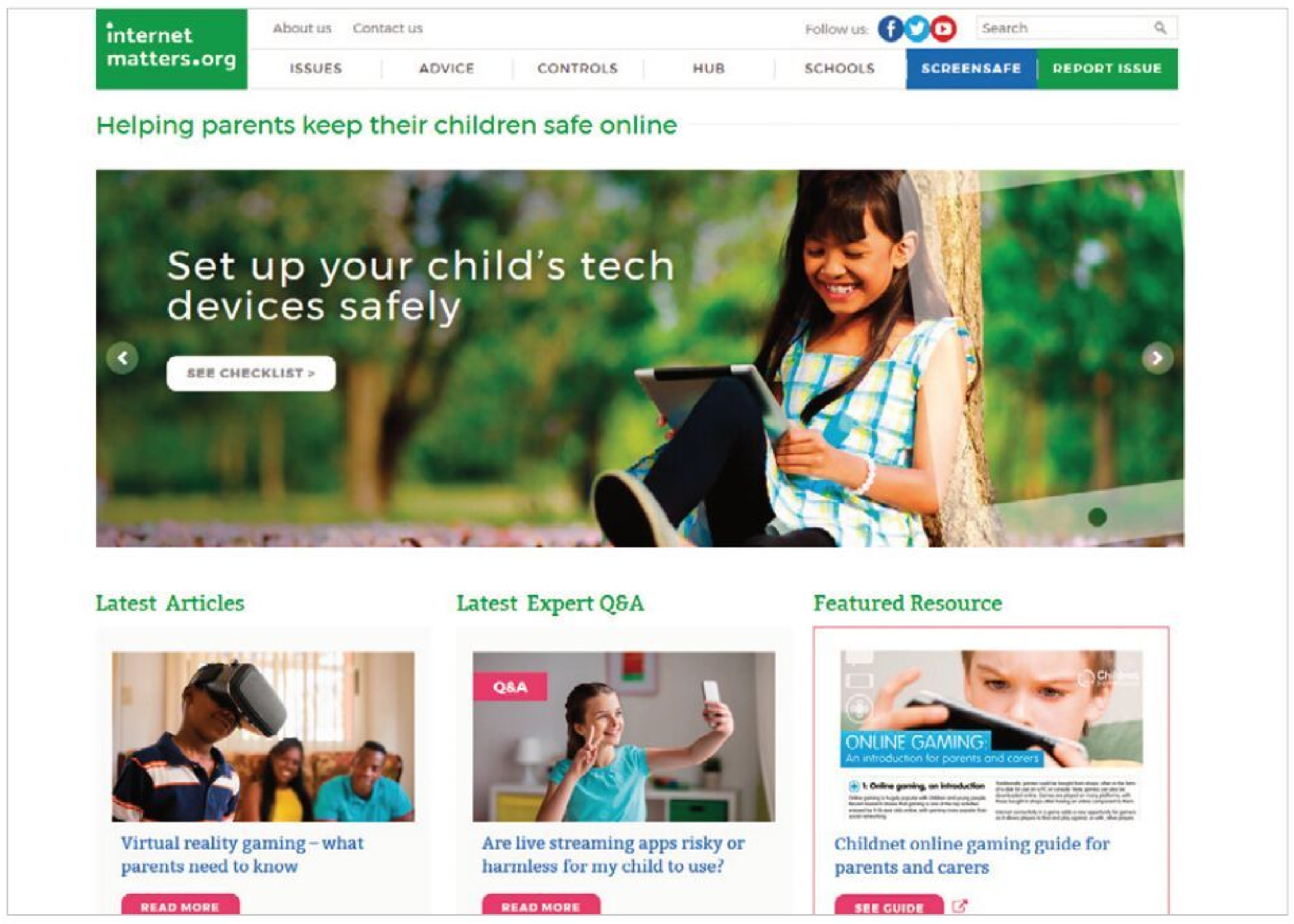
> Find out more

Welcome to Childnet International, a non-profit organisation working with others to help make the internet a great and safe place for children.

Our latest blog looks at #free internet safety resources for parents bit.ly/2uspFWZ pic.twitter.com/vs758loQT9

Keeping under fives safe online - Our guidance for parents and carers bit.ly/2usOJgF

TIP 6 Internet Matters features articles, advice, support, guidelines and tips on how to protect your children better when online. There are plenty of resources to hand for children at preschool, all the way up to teenagers at college. It's at **https://www.Internetmatters.org/**.


internet matters.org
About us
Contact us
Follow us:
Search
ISSUES
ADVICE
CONTROLS
HUB
SCHOOLS
SCREENSAFE
REPORT ISSUE
SEE CHECKLIST >
Q&A
ONLINE GAMING
An introduction for parents and carers
READ MORE
READ MORE
SEE GUIDE

Helping parents keep their children safe online

Set up your child's tech devices safely

Latest Articles

Virtual reality gaming – what parents need to know

Latest Expert Q&A

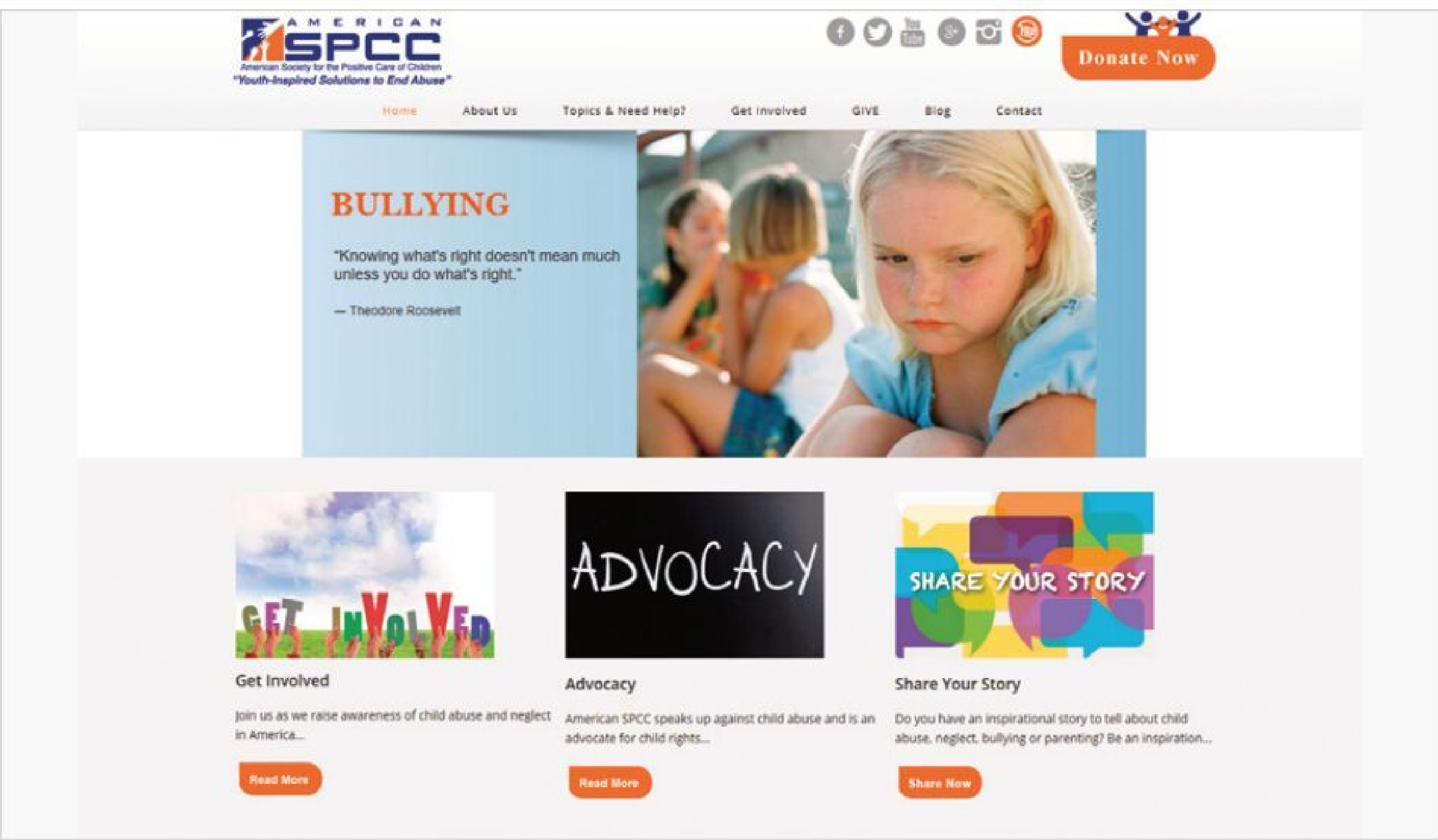
Are live streaming apps risky or harmless for my child to use?

Featured Resource

Childnet online gaming guide for parents and carers

TIP 7 To expand on the first entry in our list, local support groups are an ideal source of information and tips. Other parents and guardians going through the same considerations as yourself may well be more than happy to share any tips they have.

TIP 8 The American SPCC (Society for the Positive Care of Children) is yet another superb site that details advice on cyber bullying amongst other child protection issues. There's also a list of recommended books for you to look up. You can find the ASPCC at **http://americanspcc.org/**.


AMERICAN SPCC
American Society for the Positive Care of Children
"Youth-Inspired Solutions to End Abuse"
Donate Now
Home
About Us
Topics & Need Help?
Get Involved
GIVE
Blog
Contact
GET INVOLVED
ADVOCACY
SHARE YOUR STORY
Read More
Read More
Share Now

BULLYING

"Knowing what's right doesn't mean much unless you do what's right."

— Theodore Roosevelt

Get Involved

Join us as we raise awareness of child abuse and neglect in America...

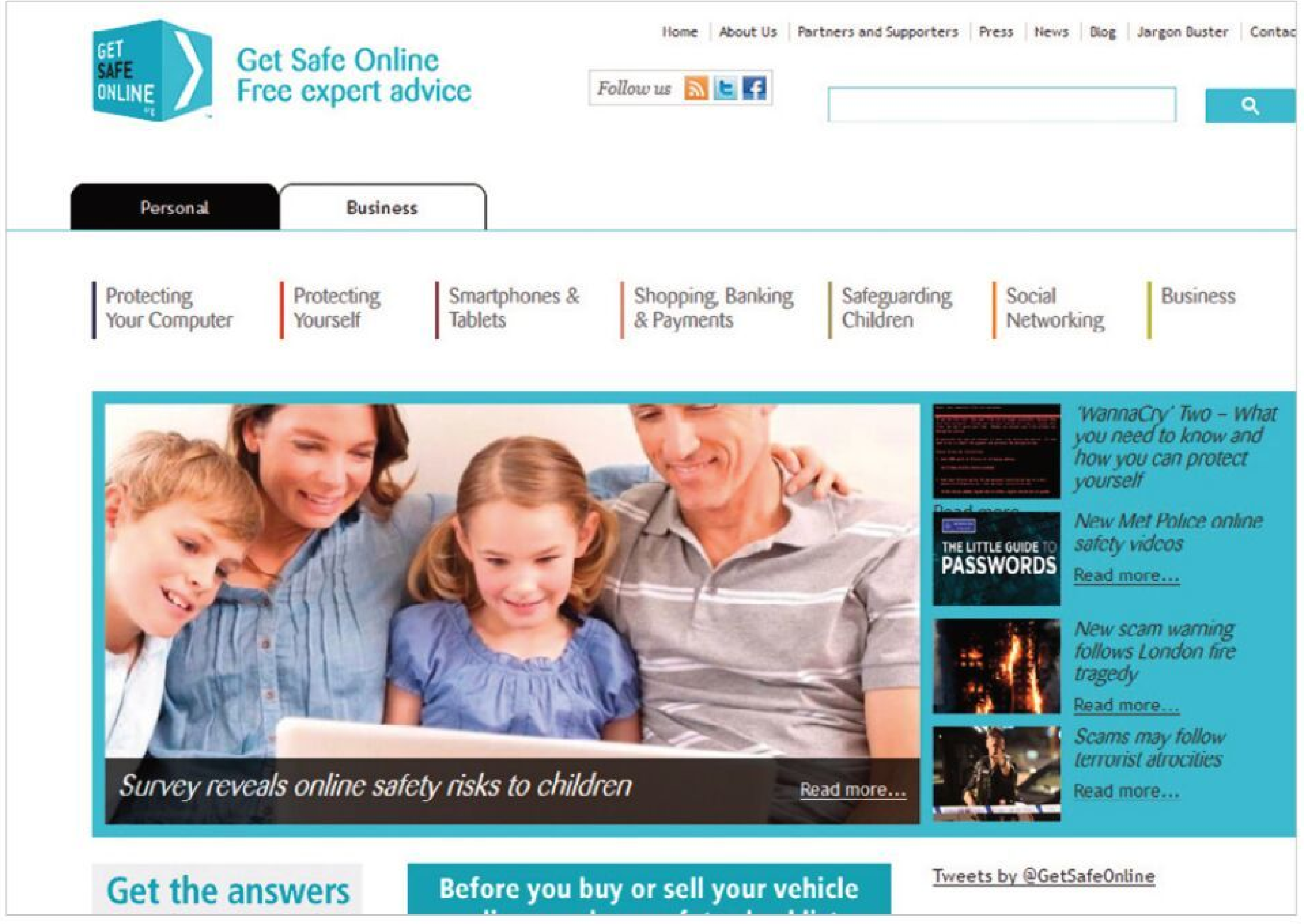
Advocacy

American SPCC speaks up against child abuse and is an advocate for child rights...

Share Your Story

Do you have an inspirational story to tell about child abuse, neglect, bullying or parenting? Be an inspiration...

TIP 9 There are some excellent resources available on the Get Safe Online website. Here you can find tips, advice and tutorials covering nearly all aspects of online child safety, including emphasis on mobile devices; there's plenty to get through. You can find it all at **https://www.getsafeonline.org/**.


GET SAFE ONLINE
Get Safe Online
Free expert advice
Home
About Us
Partners and Supporters
Press
News
Blog
Jargon Buster
Contac
Follow us
Personal
Business
Protecting Your Computer
Protecting Yourself
Smartphones & Tablets
Shopping, Banking & Payments
Safeguarding Children
Social Networking
Business
THE LITTLE GUIDE TO PASSWORDS
Read more...
Read more...
Read more...
Read more...
Get the answers
Tweets by @GetSafeOnline

Survey reveals online safety risks to children

'WannaCry' Two – What you need to know and how you can protect yourself

New Met Police online safety videos

New scam warning follows London fire tragedy

Scams may follow terrorist atrocities

Before you buy or sell your vehicle

TIP 10 Finally, consider checking out the website of, or visiting, the local police station for more information on online safety. The police have information on area professionals and child safety experts as well as further information on what to do if your child is the victim of an online threat.

POLICE
POLICE

What the Experts Say

Our next generation is heading into an ever increasingly connected, digital world. What we perceive as threats now will certainly change in a decade's time, as the technology surrounding us evolves and becomes even more integrated. What will remain important though, is online safety.

> *"We've gathered together quotes and asked child safety and security experts to have their say on the matter of online safety; as a result, here are ten examples from the professionals"*

> "Start discussing online safety at an early age."

David Emm, senior security researcher at Internet security company Kaspersky Lab.

> "Talking to your child openly and regularly is the best way to help keep them safe online."

NSPCC, Keeping Children Safe Online.

> "Follow the same rules you would follow in the real world."

Darren Anstee, director of solutions architects at network security company Arbor Networks.

> “Think before you post. Don’t upload or share anything you wouldn’t want your parents, teachers or friends seeing. Once you press send, it is no longer private. You can’t be sure who will end up seeing it”

Childline.

> “If you wouldn’t do it face to face, don’t do it online.”

Shelagh McManus, online safety advocate for security software Norton by Symantec.

> “Ask them about how they stay safe online. What tips do they have for you, where did they learn them and what is OK and not OK to share”

Childnet, Staying Safe Online.

> “You might find it helpful to start with a family discussion, to set boundaries and agree what’s appropriate.”

NSPCC, Keeping Children Safe Online.

> “Don’t be pressured to give your number out. If someone is pressuring you into giving them your number, tell someone about it such as a teacher or parent.”

Childline.

> “Set and monitor limits for the amount of daily or weekly time your children spend online gaming.”

Get Safe Online, Safeguarding Children, Gaming.

> “Don’t meet people you don’t know. Even if you get on with them online, you never know who they really are.”

Childline.

Glossary of Terms

The bewildering world of technological terms is often difficult even for experts to navigate without becoming slightly confused and we could easily dedicate an entire book just to the glossary. However, here are some of the more important terms from the world of digital security and safety.

Digital Security A-Z

Digital security and safety terms are often as clear as mud. Use this glossary whenever you come across a term you don't understand.

A

Access Control: A term used to ensure that resources are only granted to users who are entitled to them.

Active Content: Code that's embedded in a web site. When the site is accessed the code is automatically downloaded and executed.

Advanced Encryption Standard (AES): An encryption standard designed to specify an unclassified, publicly disclosed, symmetric encryption algorithm.

Asymmetric Cryptography: Public key cryptography, where algorithms use a pair of keys, one public and one private, to unlock the content protected by the encryption.

Authentication: Used by systems to confirm the identity of a user.

B

Backdoor: A tool used by hackers or system security experts to access a computer system or network, bypassing the system's usual security mechanisms.

Bandwidth: The limited amount of communications data that any channel is capable of sending or receiving in a specific time.

Biometrics: A security measure that uses physical characteristics to authenticate a user's access to a system.

Boot Sector Virus: A virus that can affect a computer as it boots, before the operating system has even loaded.

Botnet: A large number of Internet connected, infected computers that are used to flood a network or send spam message to the rest of the Internet.

Brute Force: A hacking technique that uses all possible password combinations one at a time in order to gain access to a user account or system.

C

Cipher: A cryptographic algorithm used in the encryption and decryption process.

Cookie: A file used to store information about a website that can be read should the user ever visit the site again.

Cyber Attack: An attack on a system using malware to compromise its security. Usually in order to gain access to steal information or demand a ransom.

Cyber Bullying: When an individual, or group of individuals, threaten or post negative and derogatory messages or doctored images of someone online.

D

Data Encryption Standard (DES): A popular method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used.

Decryption: The process of transforming an encrypted message into its original text form.

Demilitarised Zone (DMZ): A demilitarised zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organisation's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy. DMZ's provide either a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination.

Denial of Service (DoS): Prevention of authorised access to a system or network.

Disaster Recovery Plan (DRP): A plan of action used to restore systems in the event of a disaster.

Distributed Denial of Service (DDoS): A type of DoS attack using multiple attacking systems to amplify the amount of network traffic, thereby flooding and swamping the target systems or networks.

Domain Name System (DNS): The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy to remember 'handle' for an Internet address.

E

Encryption: The process of securing data by transforming it into something unreadable using cryptographic means.

Ethernet: Communication architecture for wired local area networks.

F

Fingerprinting: Used by hackers and security experts to send packets to a system in order to see how it responds, usually to determine the operating system and security measures.

Firewall: A hardware or software layer designed to prevent unauthorised access to or from a computer or network to another computer or network.

Flooding: A malware attack that causes an eventual failure of a system by bombarding it with a continuous stream of data.

G

Gateway: A network point that acts as the door into another network.

H

Hacker: Someone who violates or circumvents a computer security measure. Can be used for malicious purposes or legitimately to test a system's vulnerabilities.

HTTP: Hypertext Transfer Protocol, the protocol used by the World Wide Web (Internet) that defines how messages are sent, received and read by browsers and other connected software layers.

HTTPS: Hypertext Transfer Protocol Secure, an encrypted and far more secure version of HTTP.

I

Internet Protocol Address (IP): A standard used by servers and machines to connect to each other and form an individual identity for each connected device.

Internet Service Provider (ISP): A company that provides Internet access to businesses and residential addresses.

IP Spoofing: A form of attack where a device provides a false IP address to a server or network.

K

Key Logger: A type of malware that can record key presses as a text file and send that file to a remote source. Once obtained, the hacker can then see what keys you've pressed.

L

Local Area Network (LAN): Communications network linking multiple devices in a defined, limited location, such as a home or office.

Logic Bomb: A type of malware that's dormant until a predefined time when it explodes and runs or injects malicious code into a system.

M

Malicious Code: Software that's designed to circumvent security measures and gain unauthorised access to a system.

Malware: A generic term to describe different types of malicious code.

N

Network: A group of linked computers or devices that can share resources and communicate with each other.

P

Password: A secret security measure used to access a protected resource and authenticate access.

Phishing: A method used by cyber criminals to obtain information from a user by baiting them with fake emails or messages.

PIN: Personal Identification Number, used as a form of authentication access to a system, resource or user account.

R

Ransomware: A type of malware that locks, or encrypts, all files on a system until a ransom is paid and the unlock code is entered.

Rootkit: A set of tools used by a hacker to mask their intrusion and obtain administrator access to a system.

S

Sandbox: A system architecture designed to test code in a secure and safe environment without it affecting the host system.

Spoofing: An attempt to gain unauthorised access.

Spyware: A type of malware that spies on a user's activities or system and reports back to a remote system.

T

Trojan Horse: A type of malware designed as a useful program but in reality hides some malicious code.

Two-Factor Authentication: Authorisation of access to a system or resource through a username/password combination as well as another form of authorisation, such as a PIN code.

V

Virus: A type of malware designed for multiple purposes to spread and infect as many computer systems as possible. Usually destructive but can be used to grind a system to a halt by using up all of its available resources.

VPN: Virtual Private Network, a secure tunnel between two systems using advanced encryption methods to protect the communications between systems.

W

Wi-Fi: A wireless network standard between connected systems.

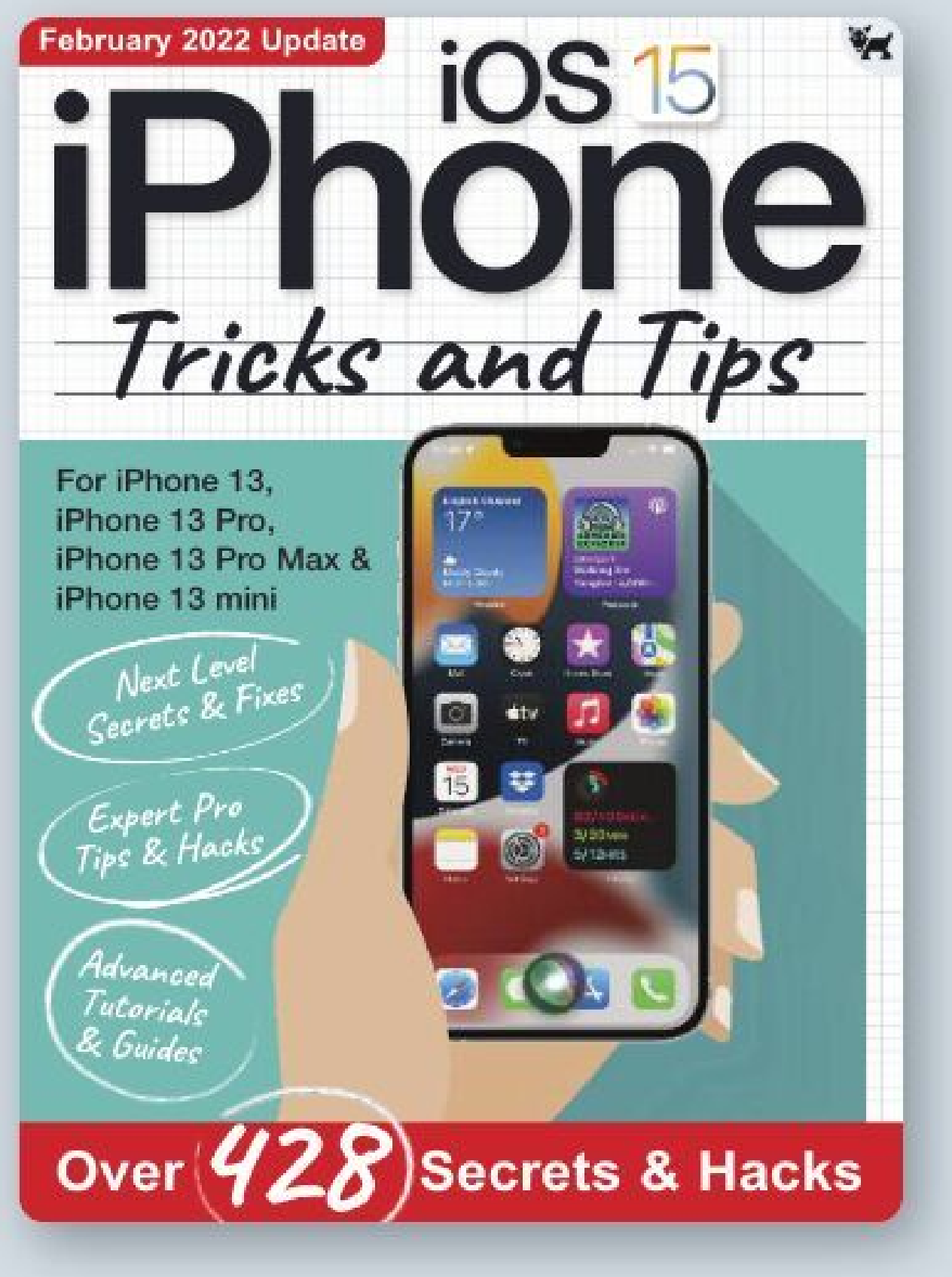
Worm: A type of malware that can replicate itself and spread through other systems consuming resources and contents destructively.

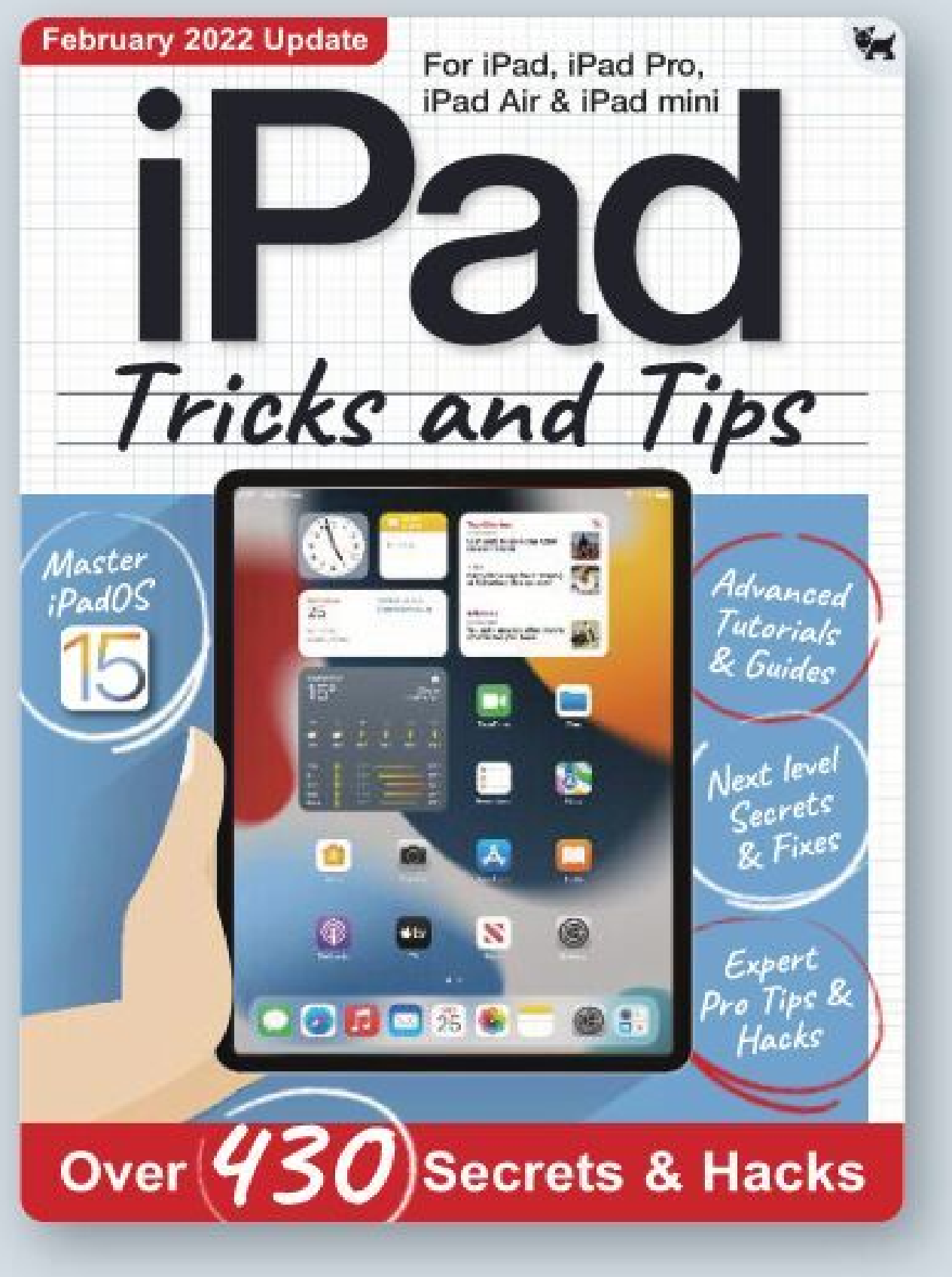
Z

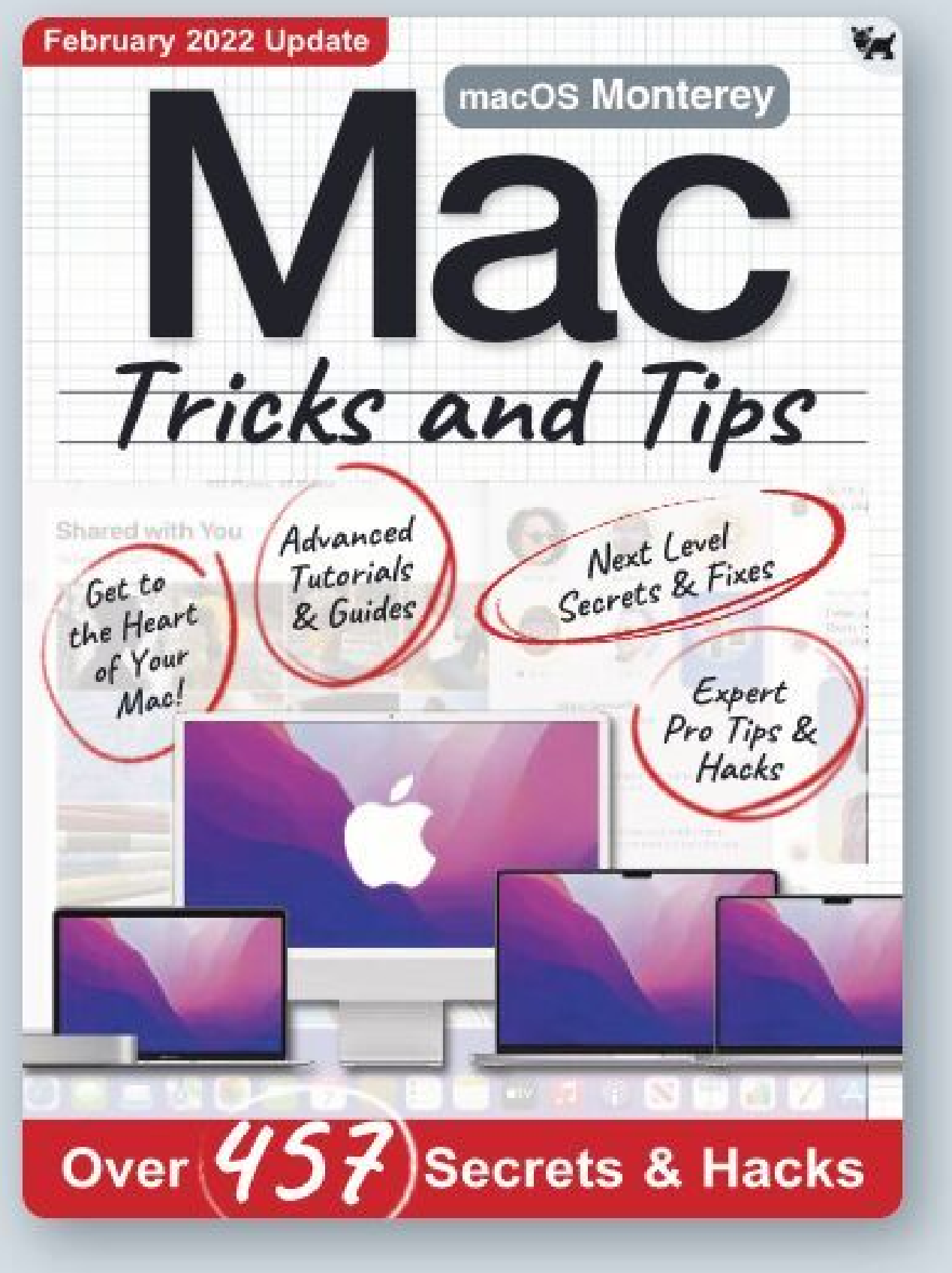
Zero Day: Described as the day a new security vulnerability is discovered, one that has no fix or patch yet to stop it.

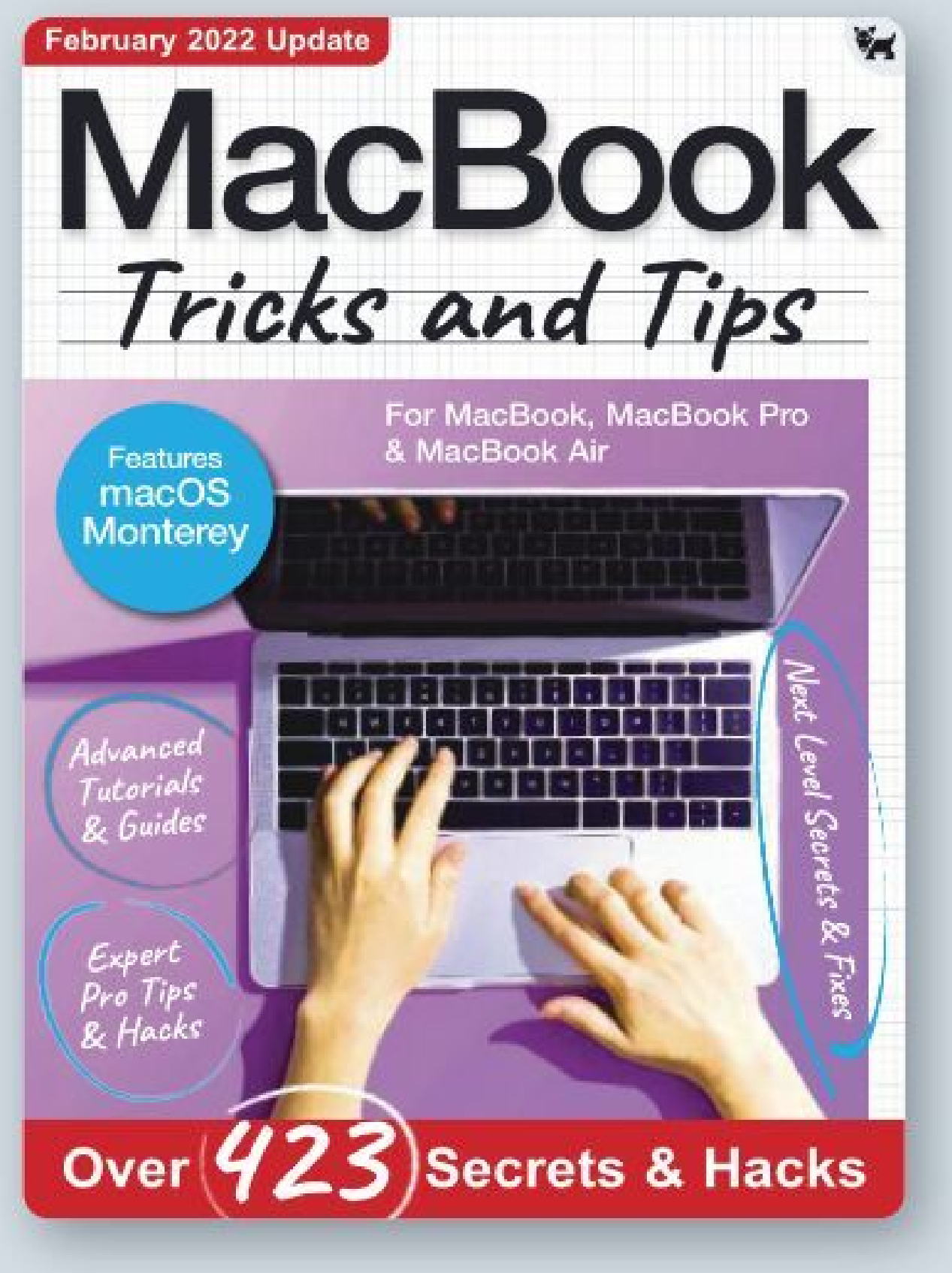
Zombie(s): A computer that's infected with malware and connected to a network or the Internet and used to spread its infection to other computers. Used also to describe an attack on other systems by hoards of zombie computers.

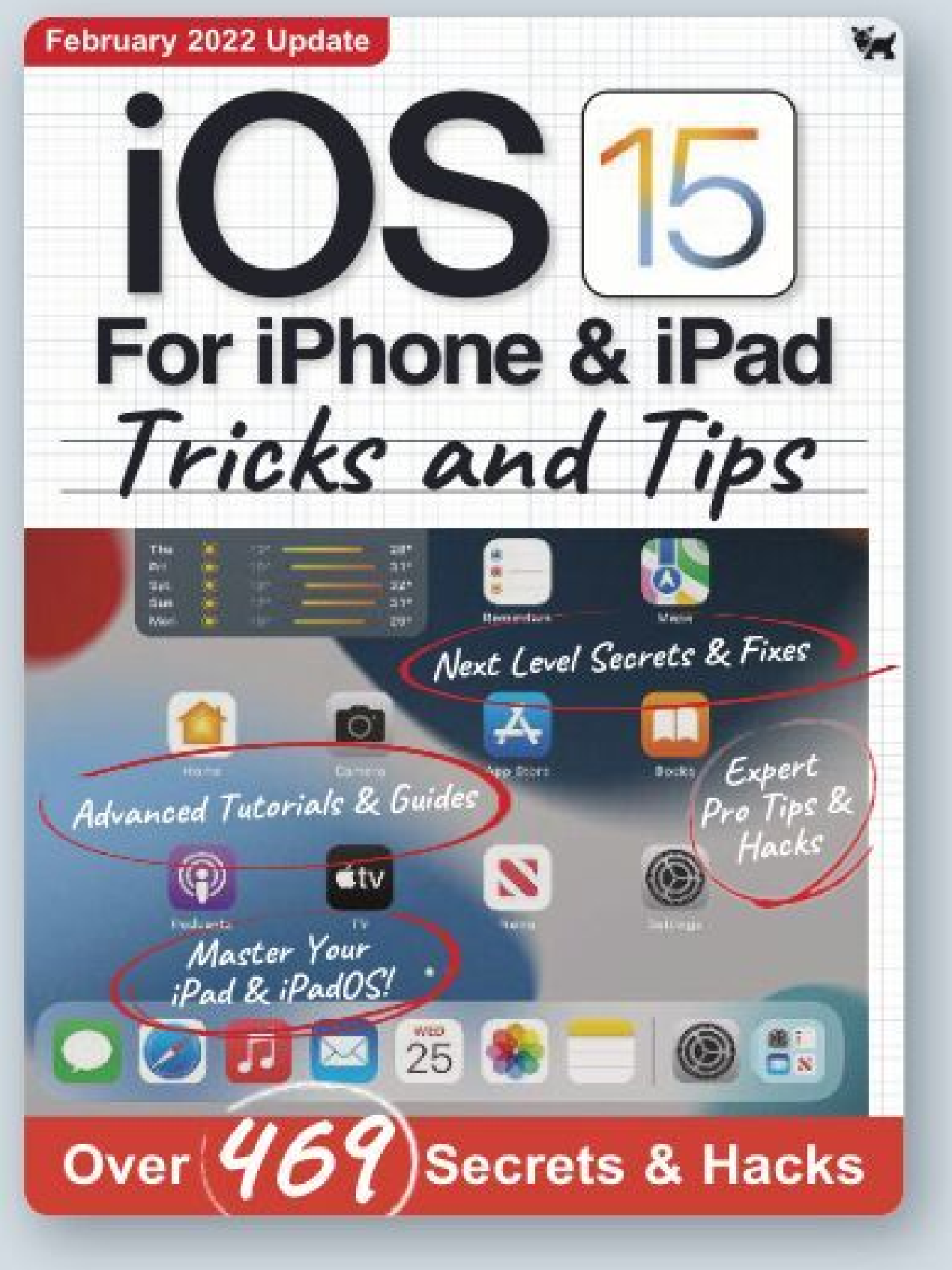
Read More Tricks and Tips

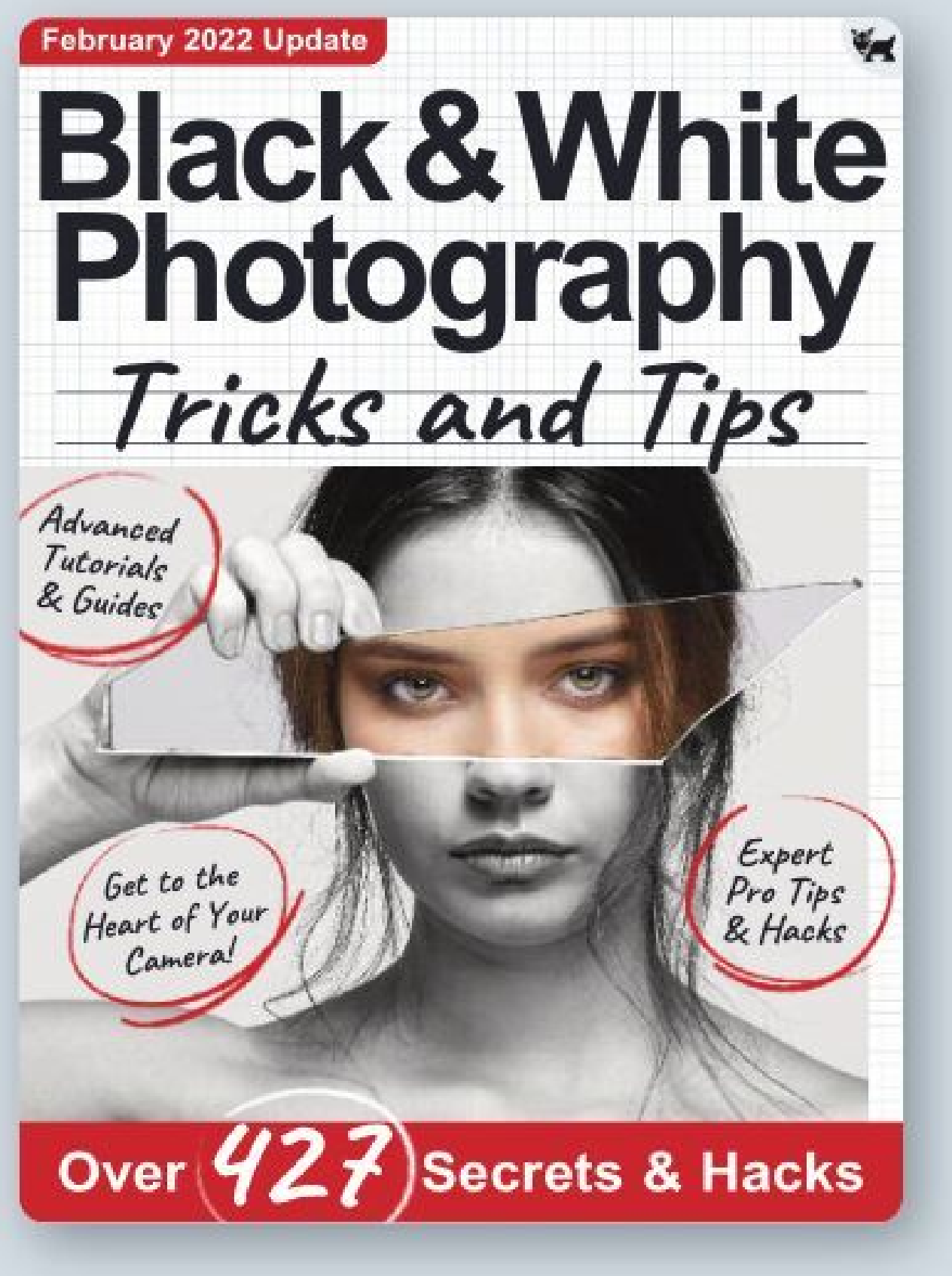

February 2022 Update
iOS 15 iPhone
Tricks and Tips
Over 428 Secrets & Hacks

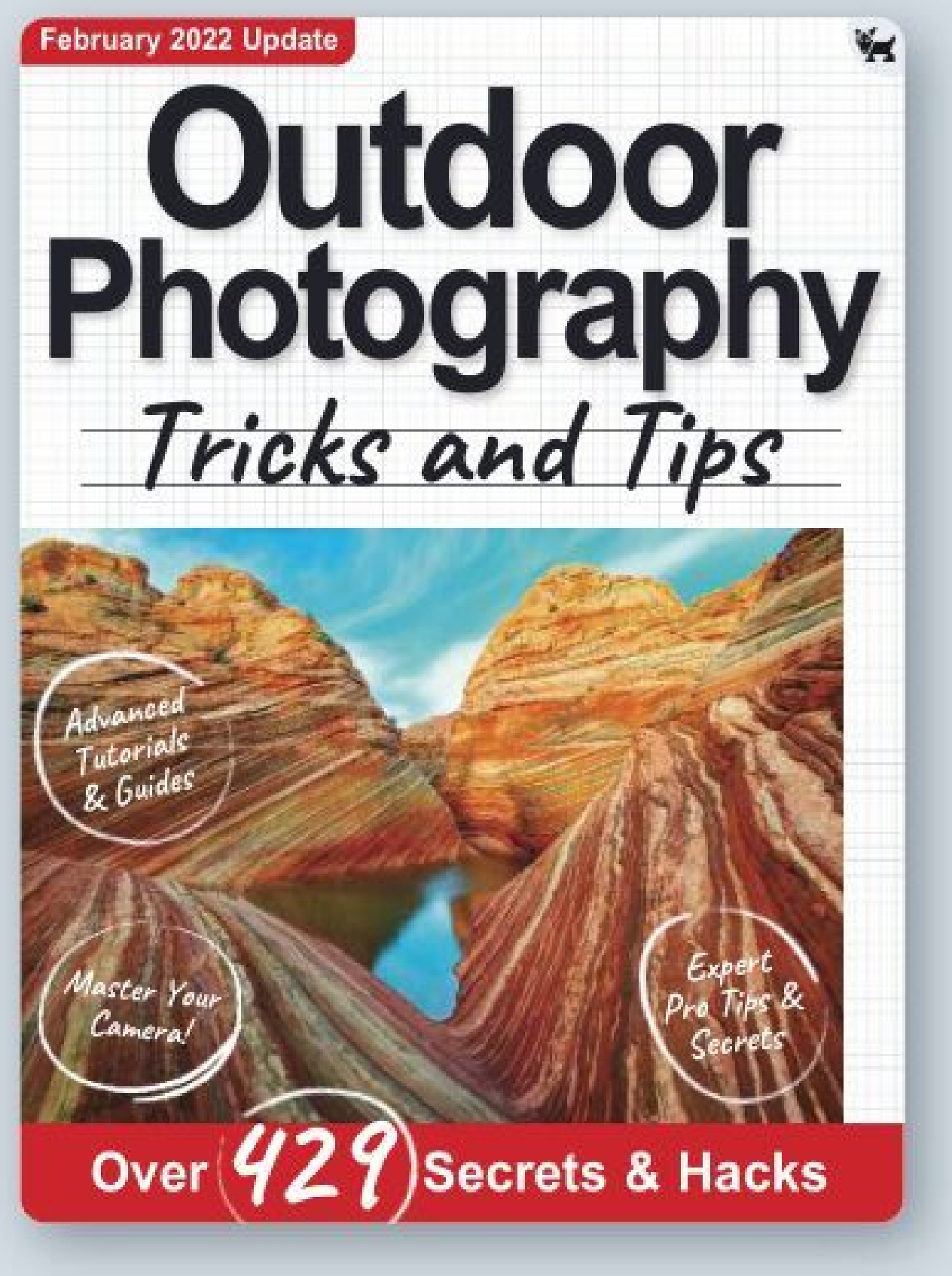

February 2022 Update
iPad
Tricks and Tips
Over 430 Secrets & Hacks

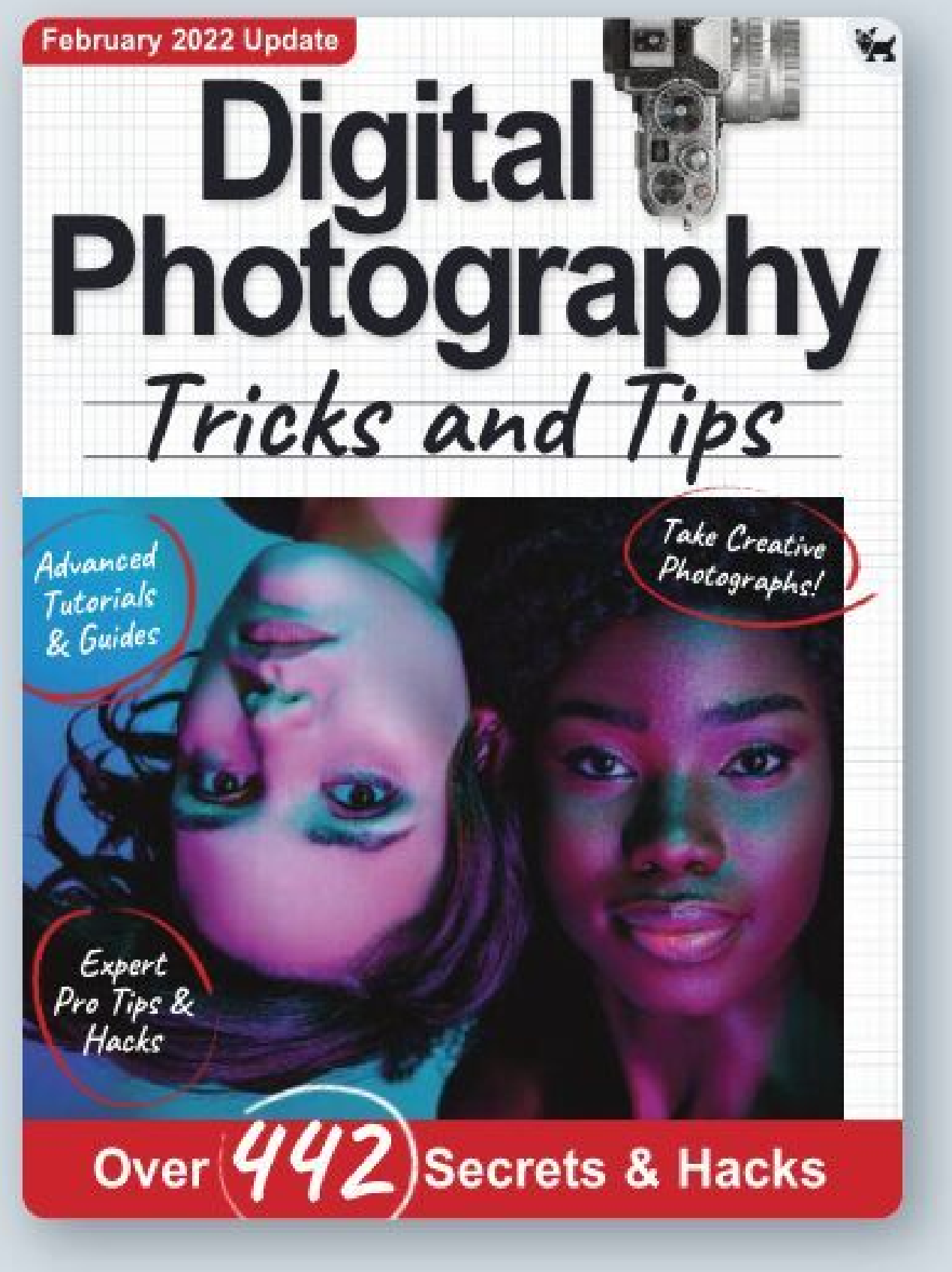

February 2022 Update
macOS Monterey
Mac
Tricks and Tips
Over 457 Secrets & Hacks

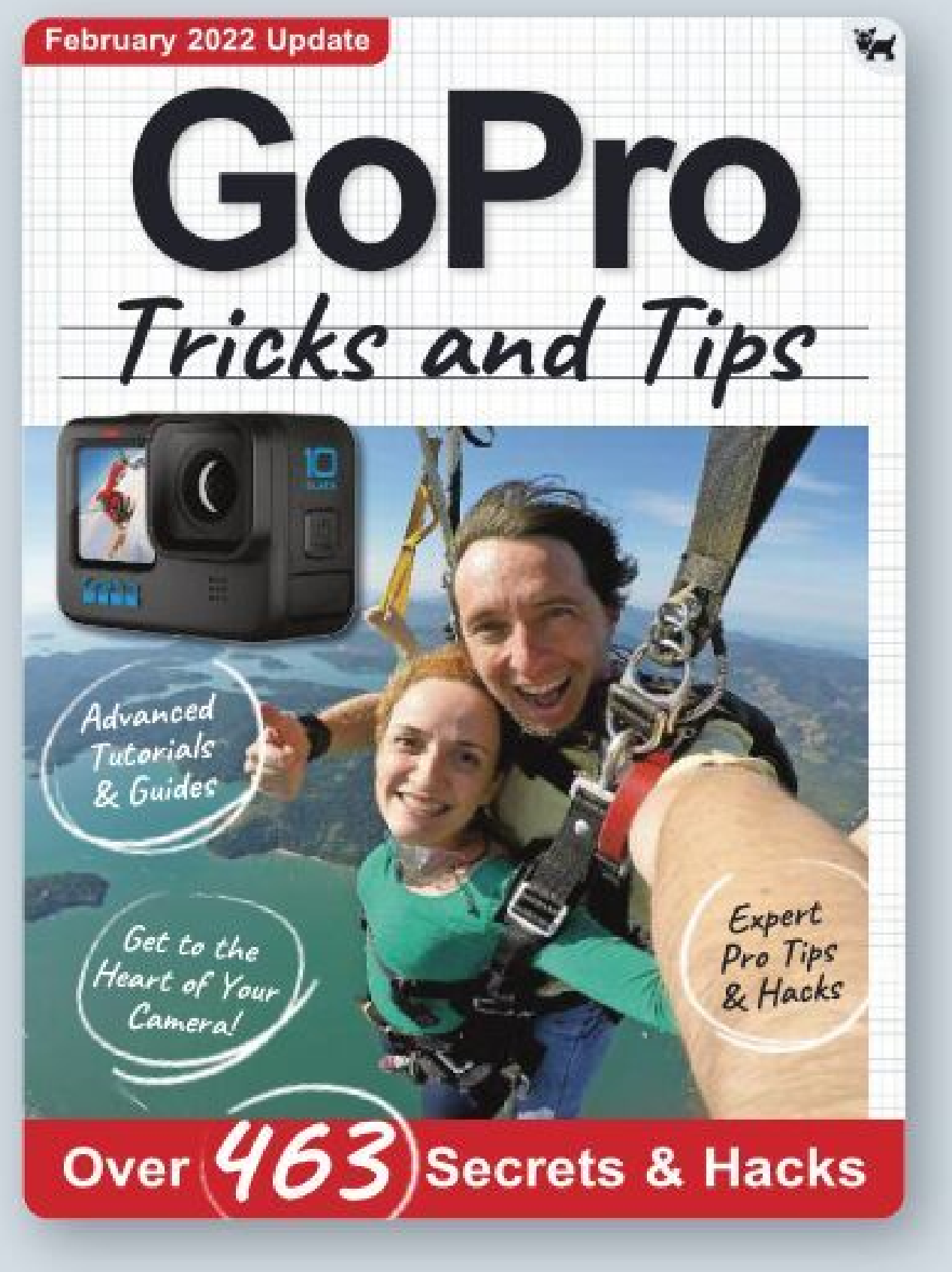

February 2022 Update
MacBook
Tricks and Tips
Over 423 Secrets & Hacks

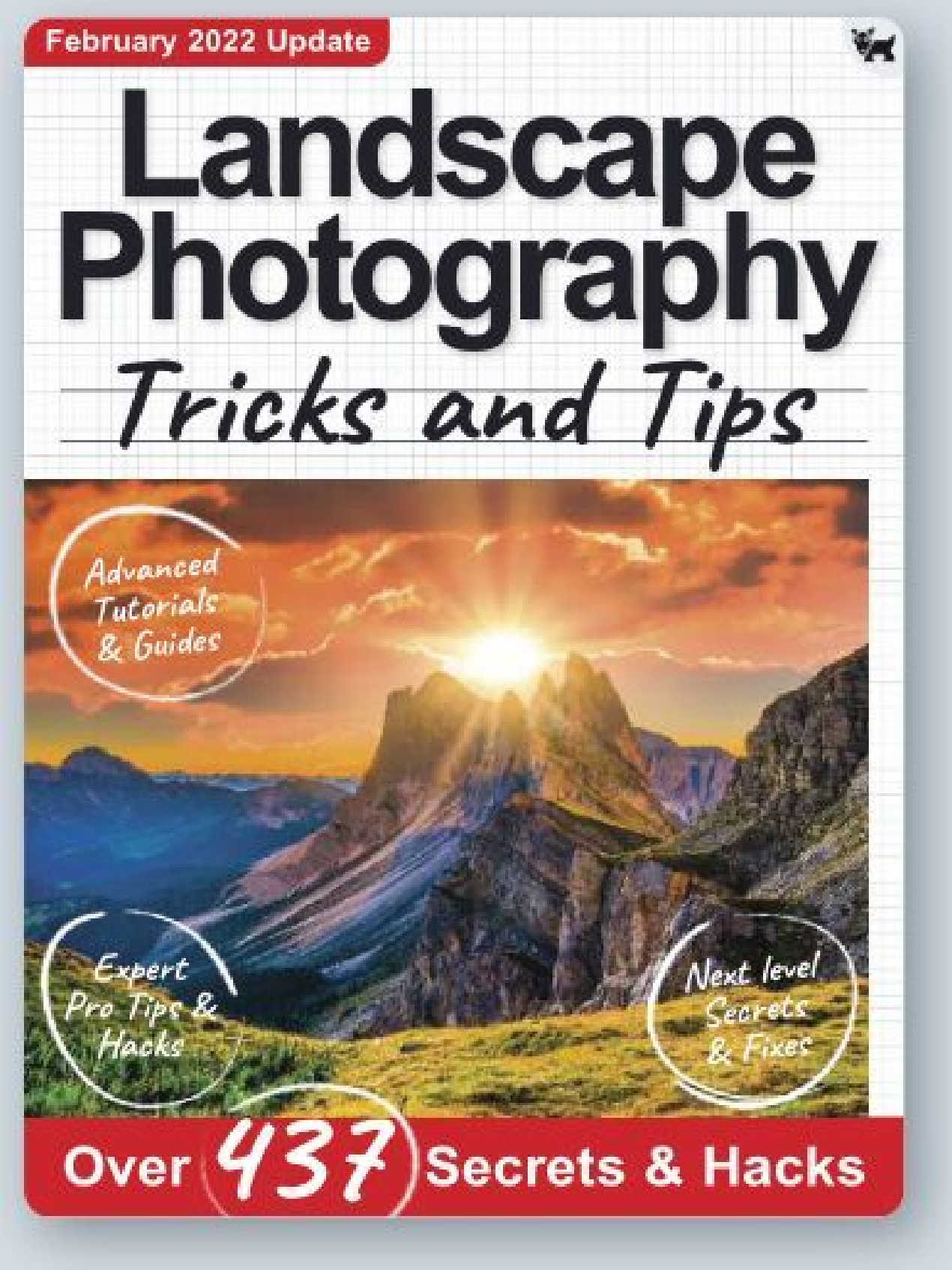

February 2022 Update
iOS 15
For iPhone & iPad
Tricks and Tips
Over 469 Secrets & Hacks

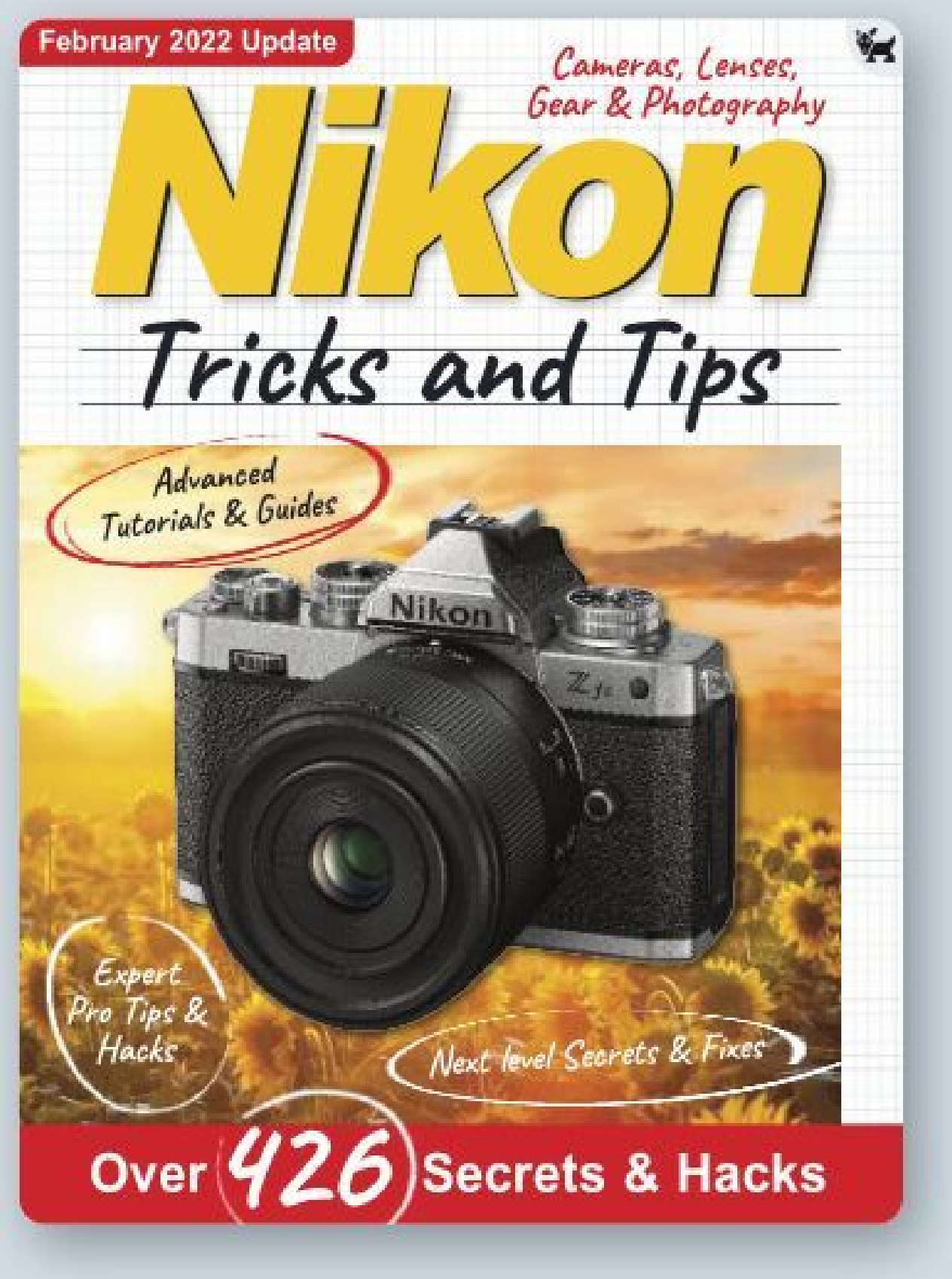

February 2022 Update
Black & White Photography
Tricks and Tips
Over 427 Secrets & Hacks

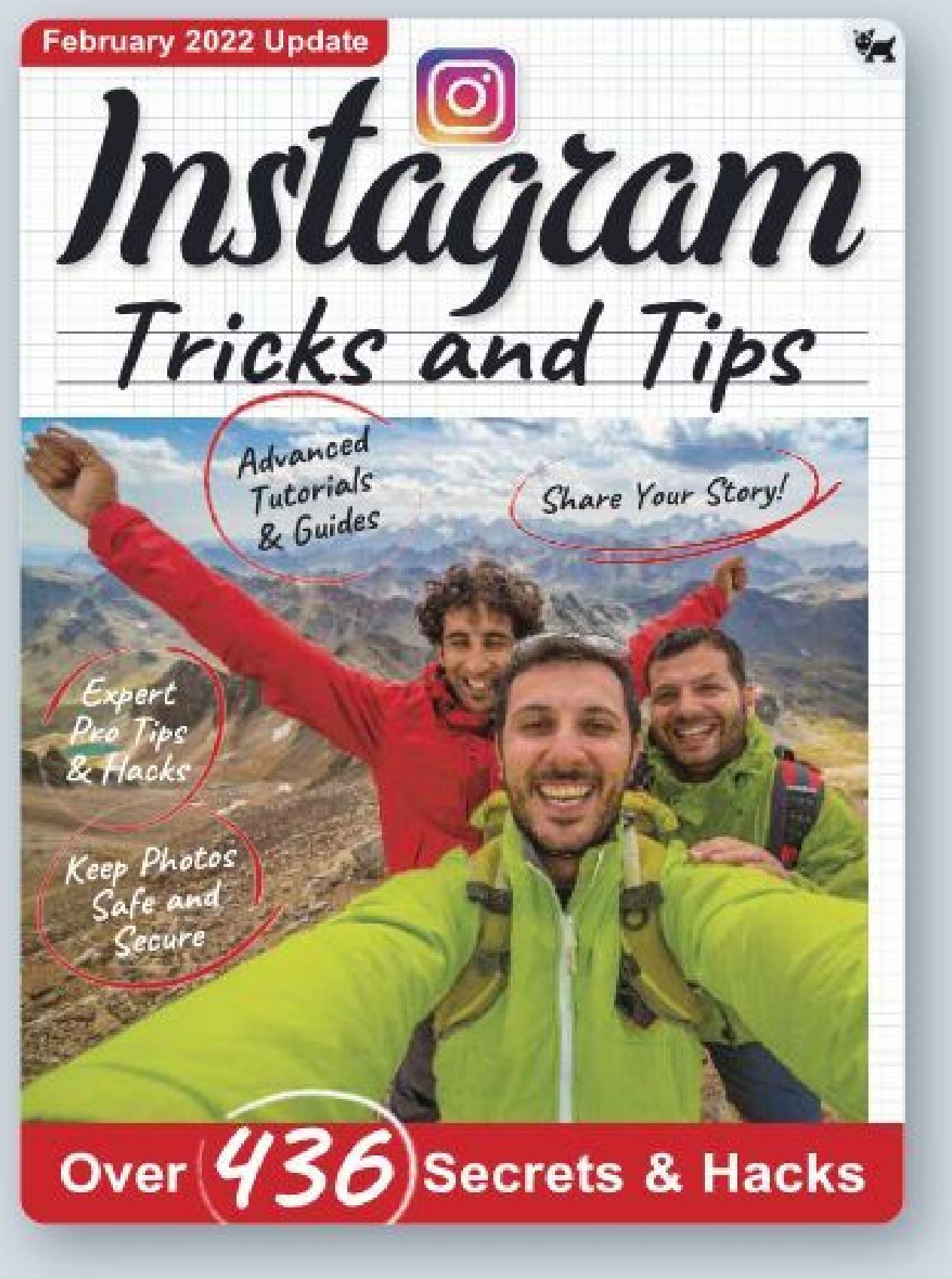

February 2022 Update
Outdoor Photography
Tricks and Tips
Over 429 Secrets & Hacks

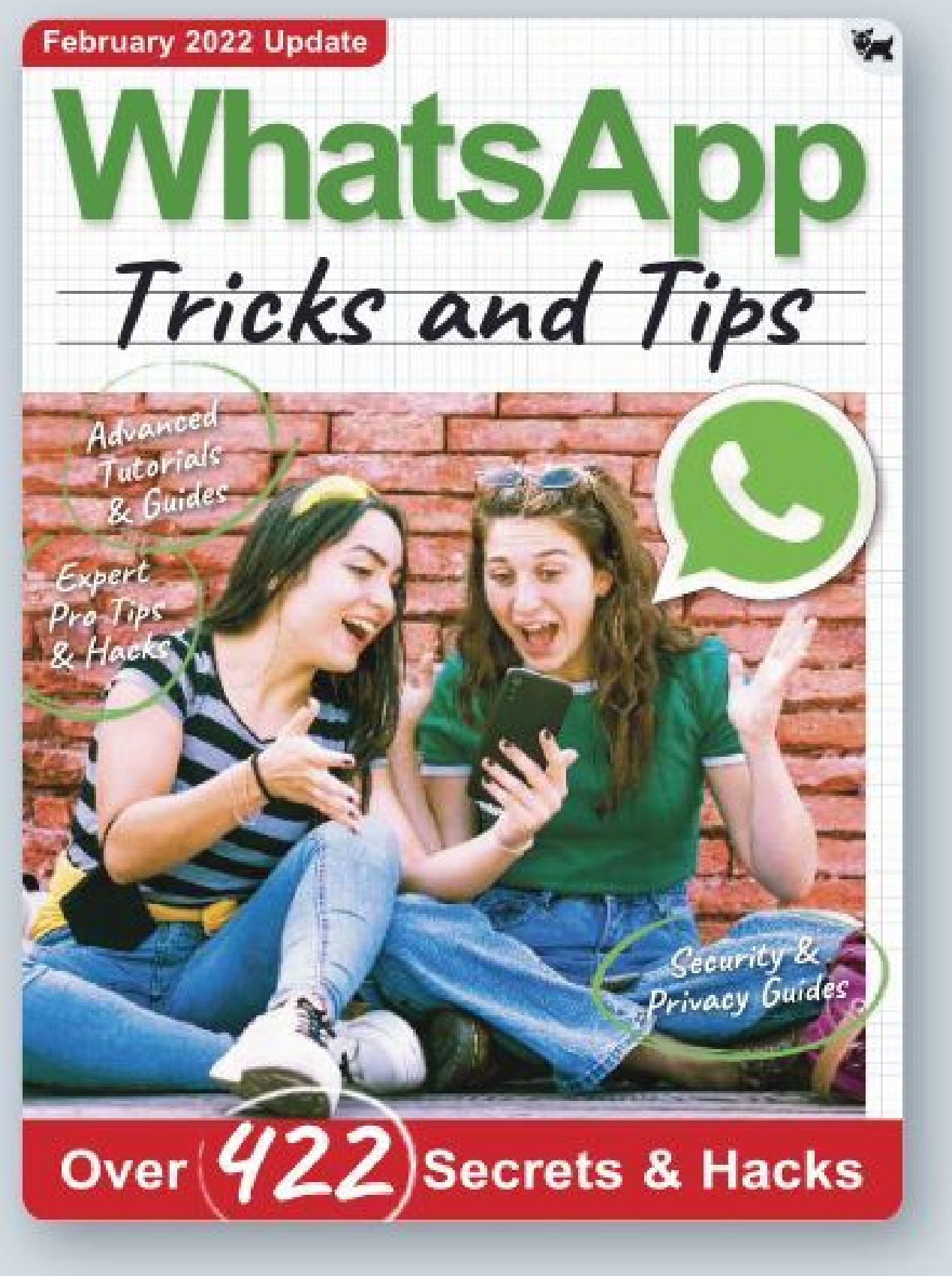

February 2022 Update
Digital Photography
Tricks and Tips
Over 442 Secrets & Hacks

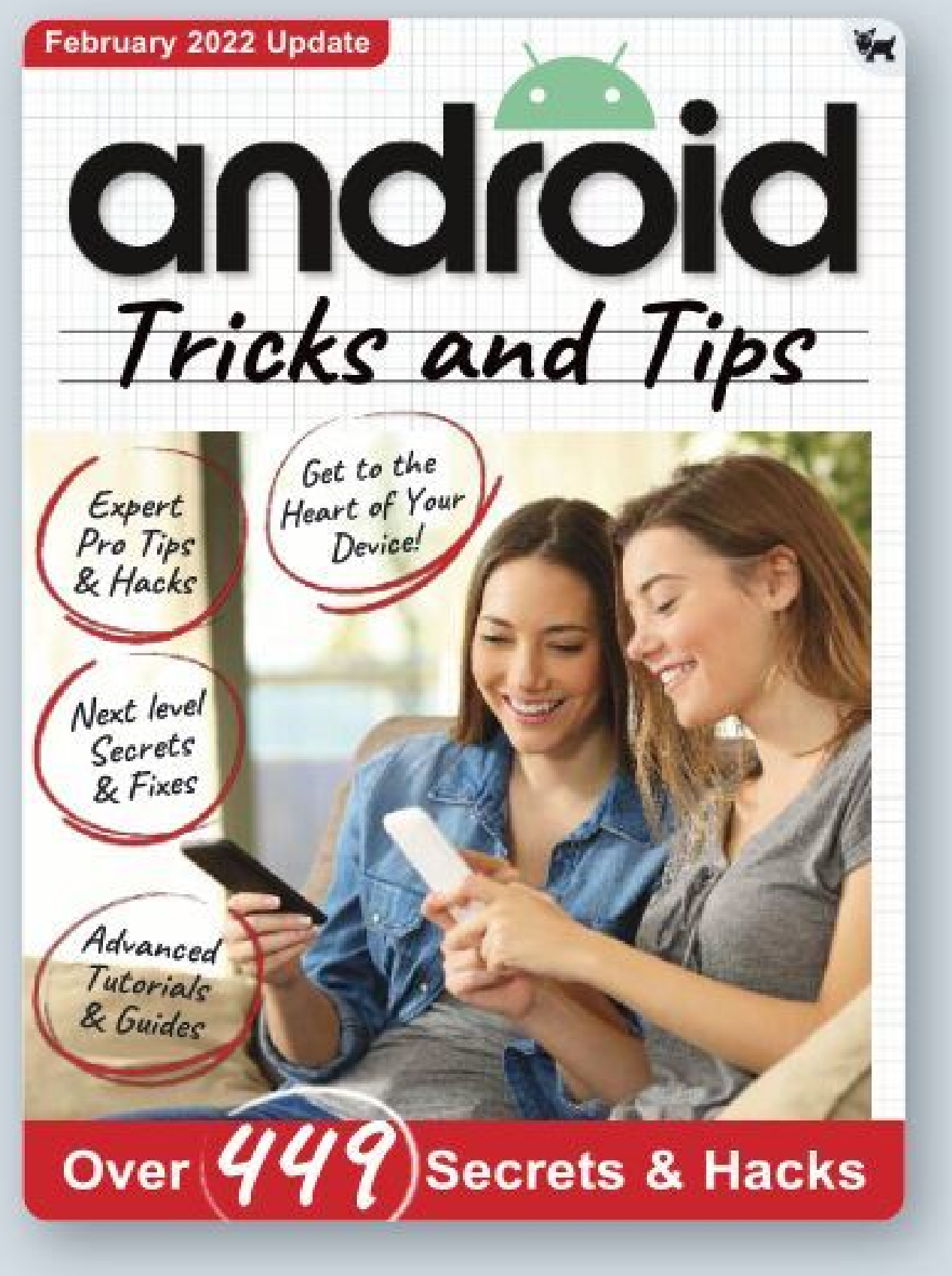

February 2022 Update
GoPro
Tricks and Tips
Over 463 Secrets & Hacks

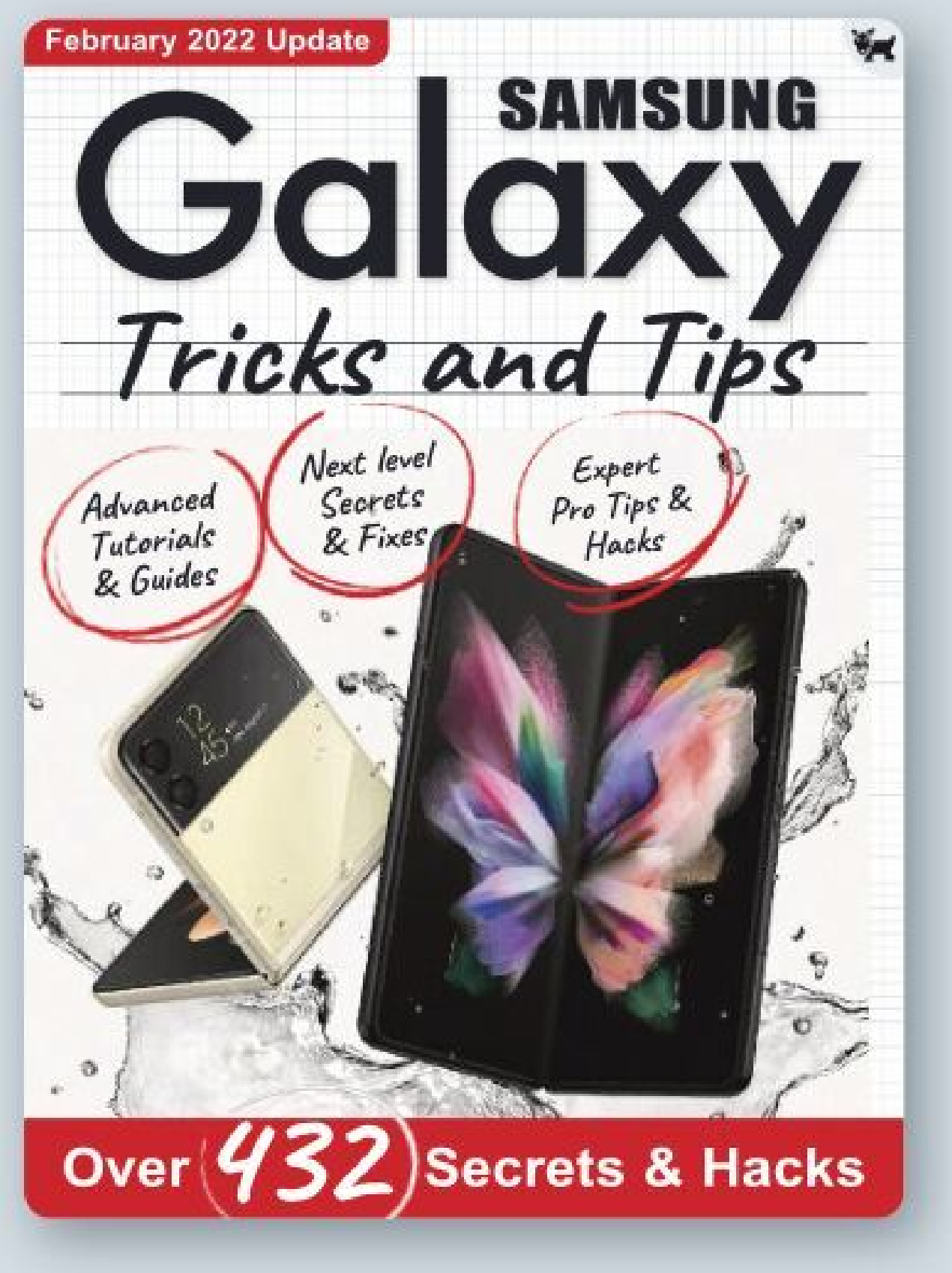

February 2022 Update
Landscape Photography
Tricks and Tips
Over 437 Secrets & Hacks

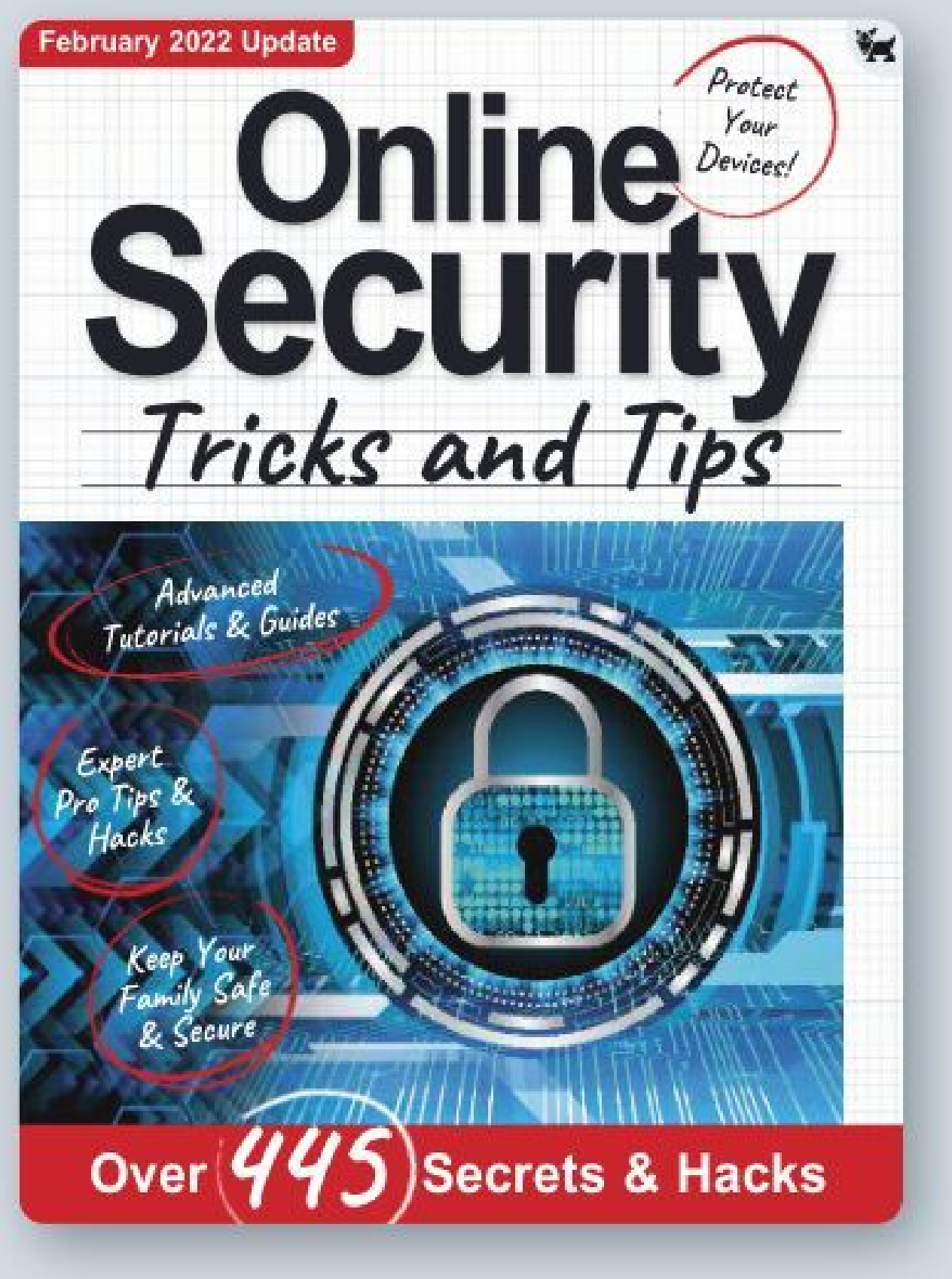

February 2022 Update
Nikon
Tricks and Tips
Over 426 Secrets & Hacks

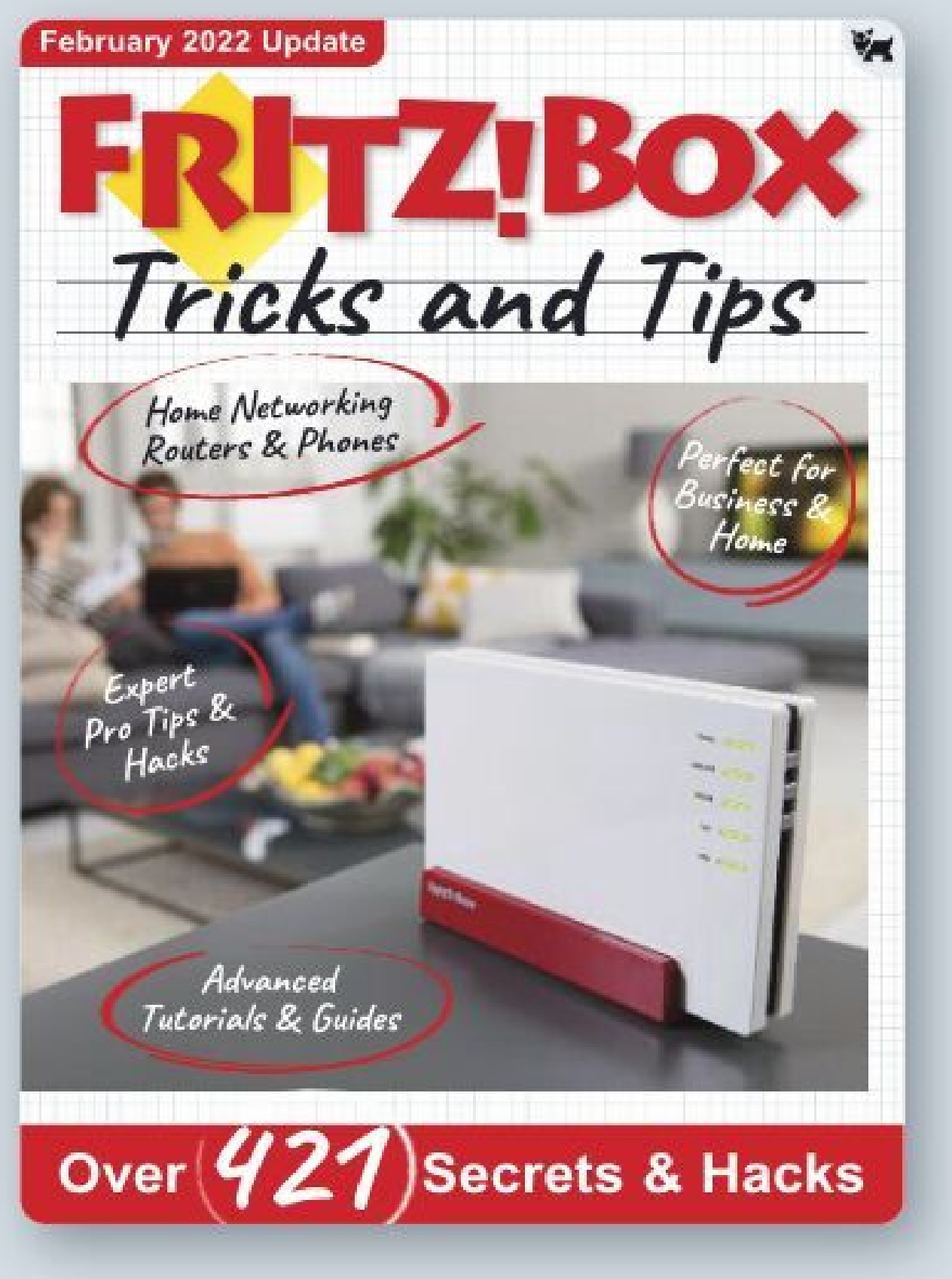

February 2022 Update
Instagram
Tricks and Tips
Over 436 Secrets & Hacks

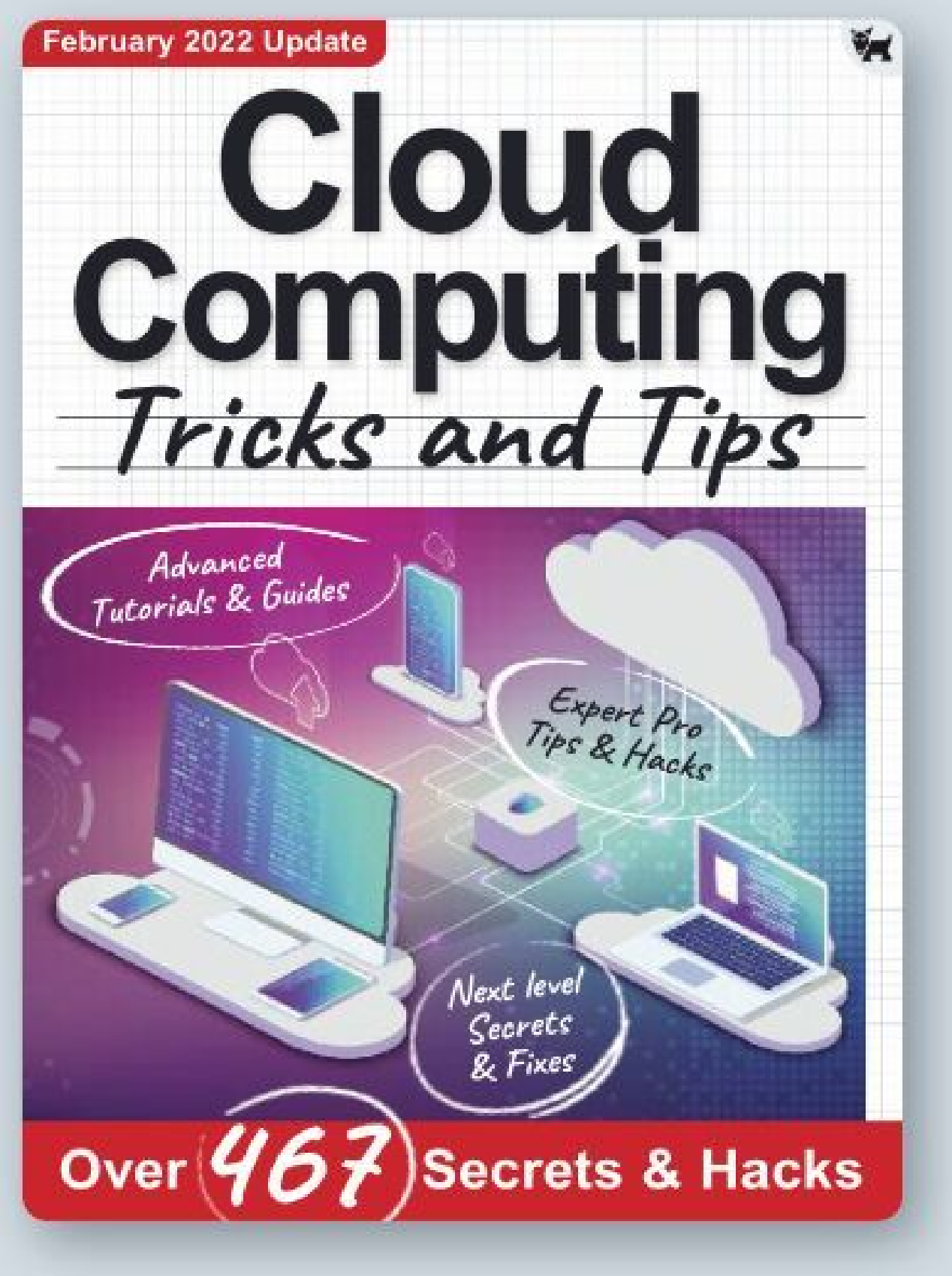

February 2022 Update
WhatsApp
Tricks and Tips
Over 422 Secrets & Hacks

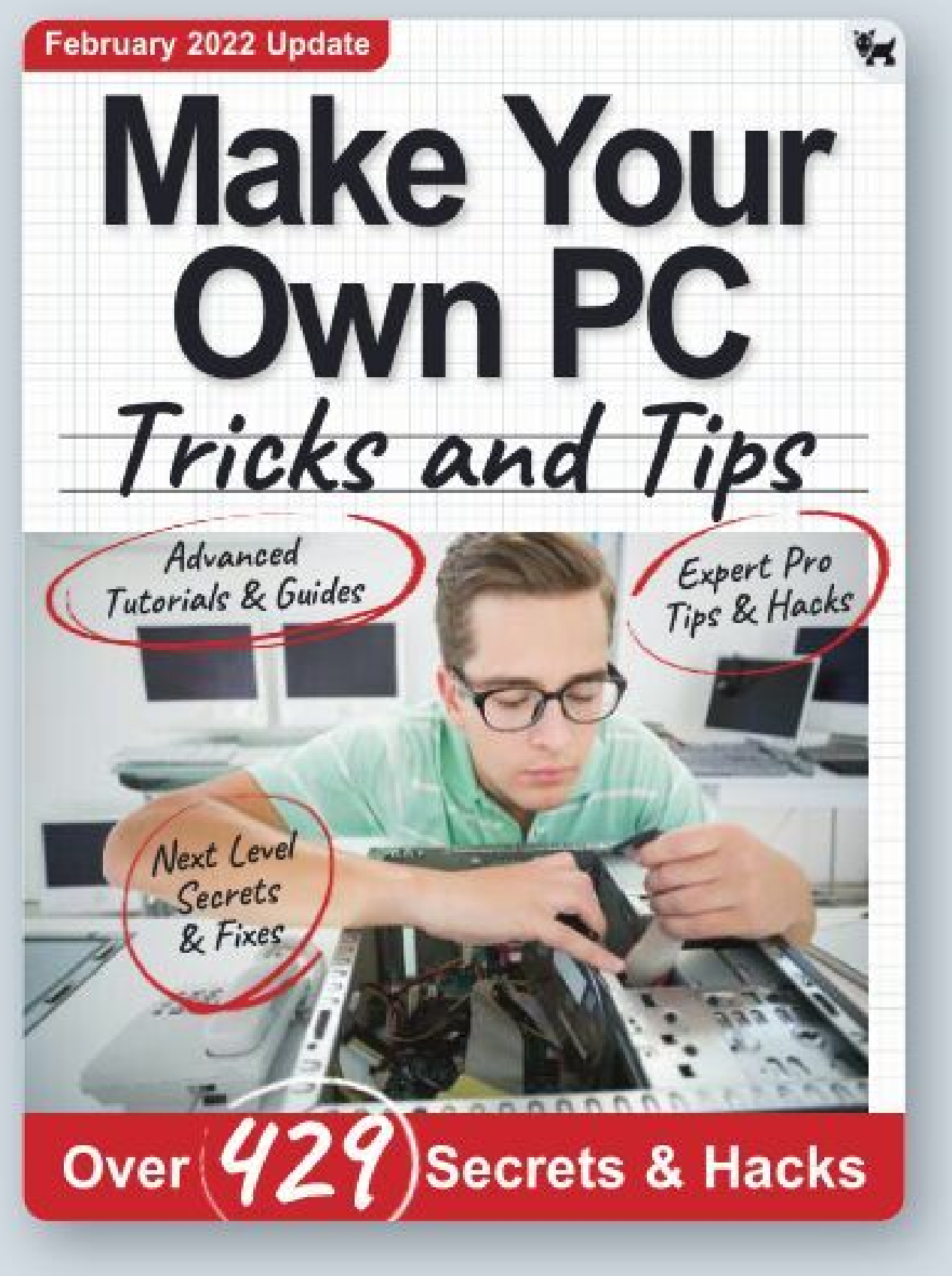

February 2022 Update
android
Tricks and Tips
Over 449 Secrets & Hacks

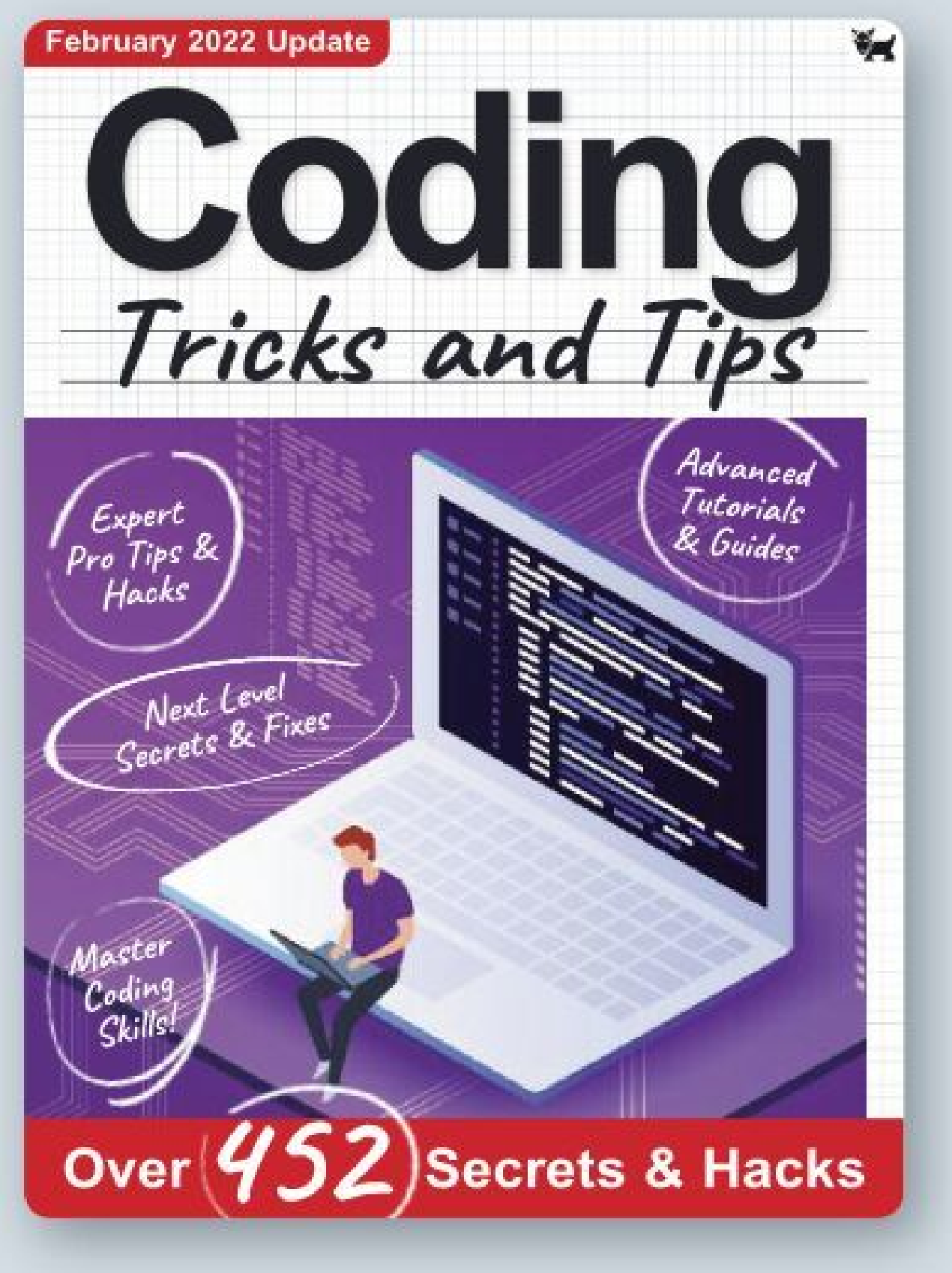

February 2022 Update
Samsung Galaxy
Tricks and Tips
Over 432 Secrets & Hacks


February 2022 Update
Online Security
Tricks and Tips
Over 445 Secrets & Hacks

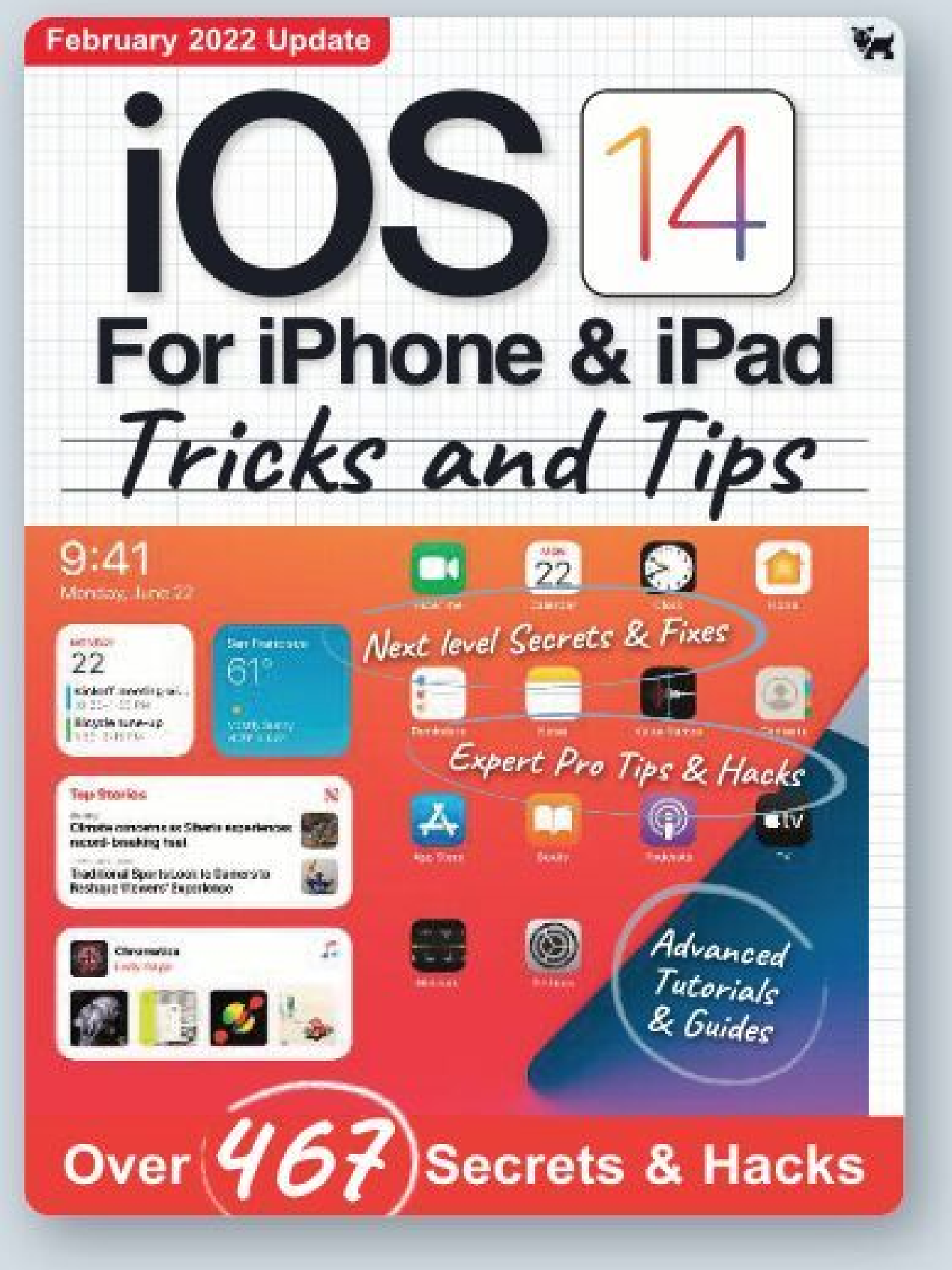

February 2022 Update
FRITZ!Box
Tricks and Tips
Over 421 Secrets & Hacks

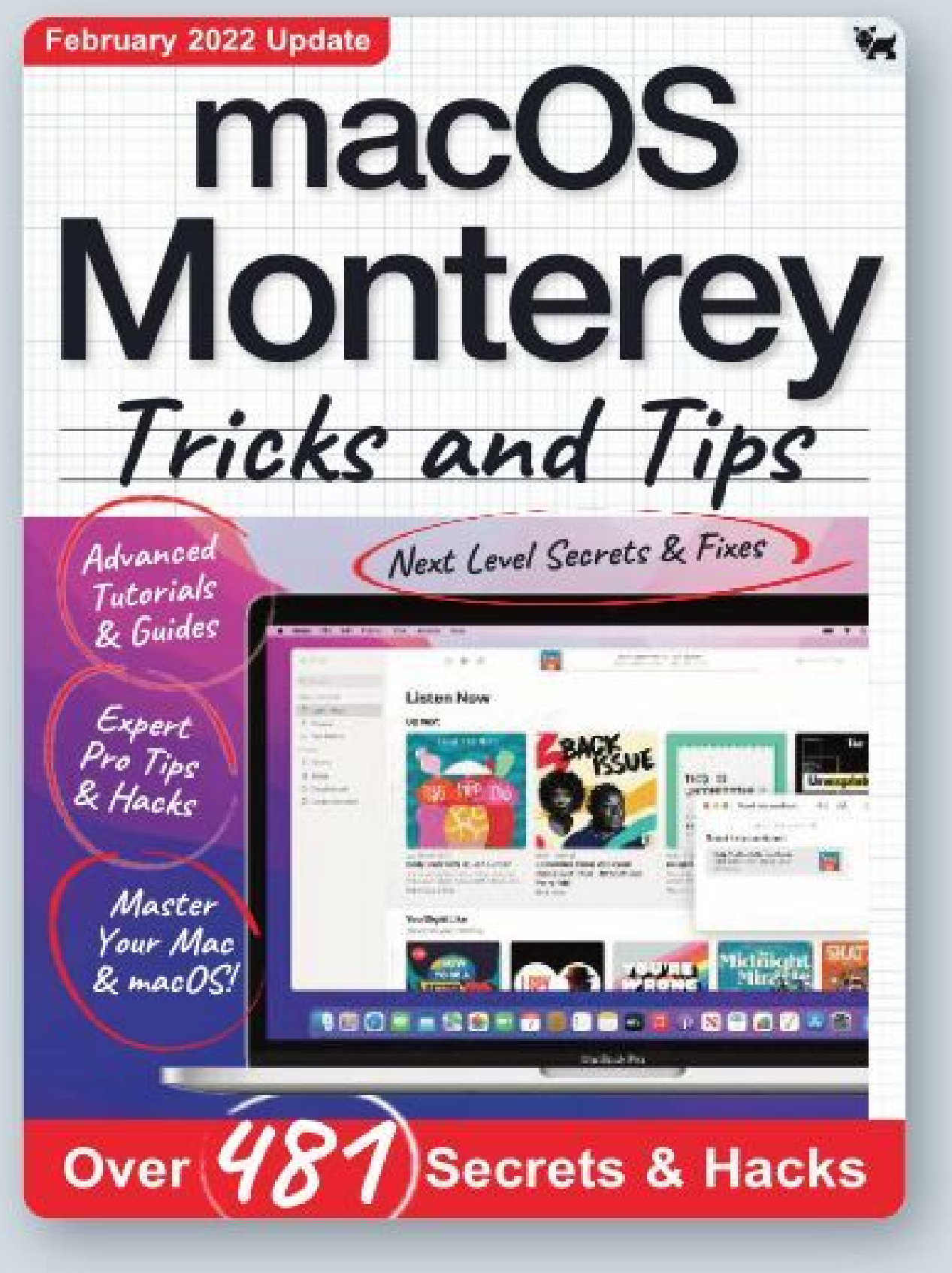

February 2022 Update
Cloud Computing
Tricks and Tips
Over 467 Secrets & Hacks

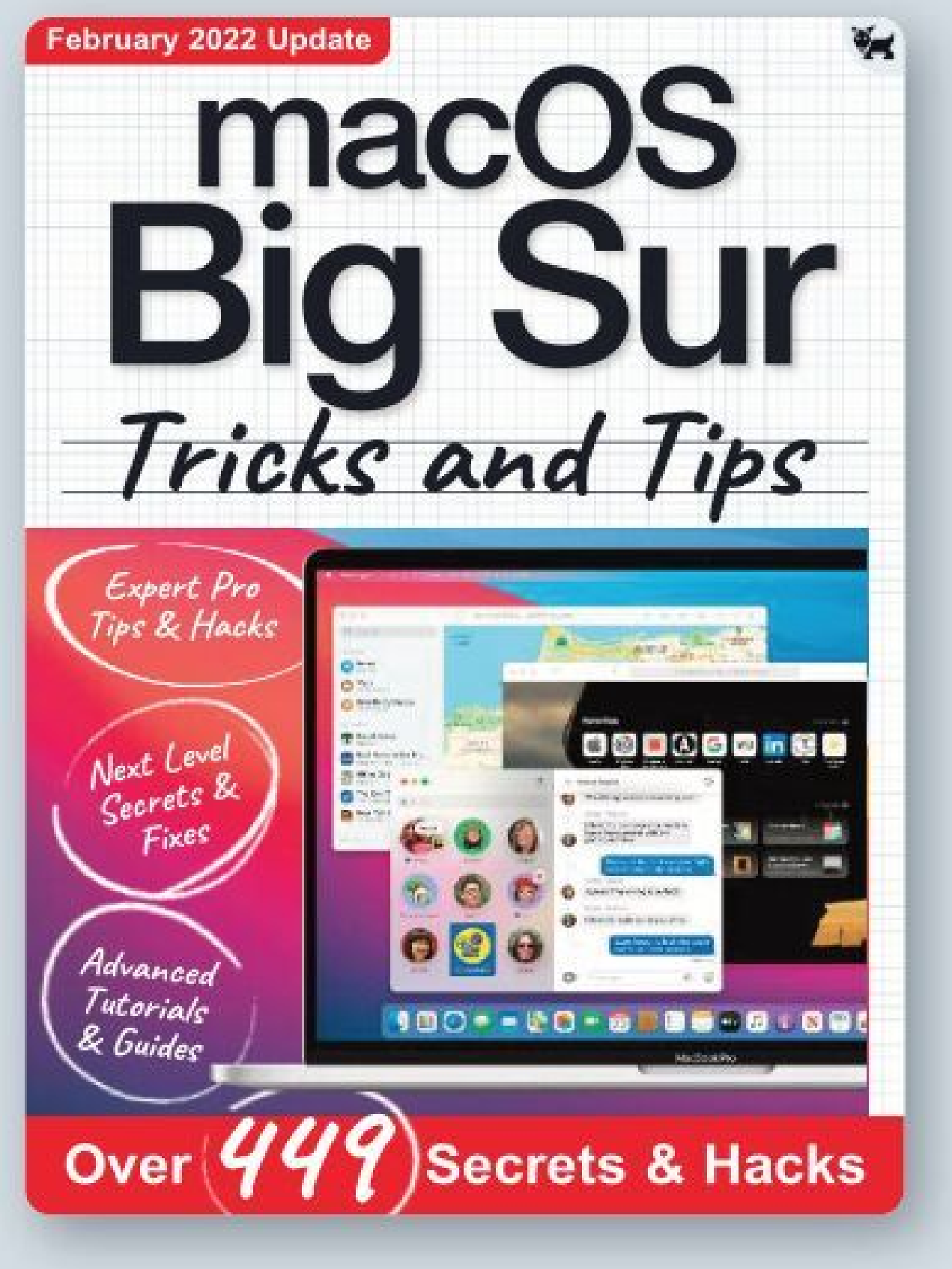

February 2022 Update
Make Your Own PC
Tricks and Tips
Over 429 Secrets & Hacks

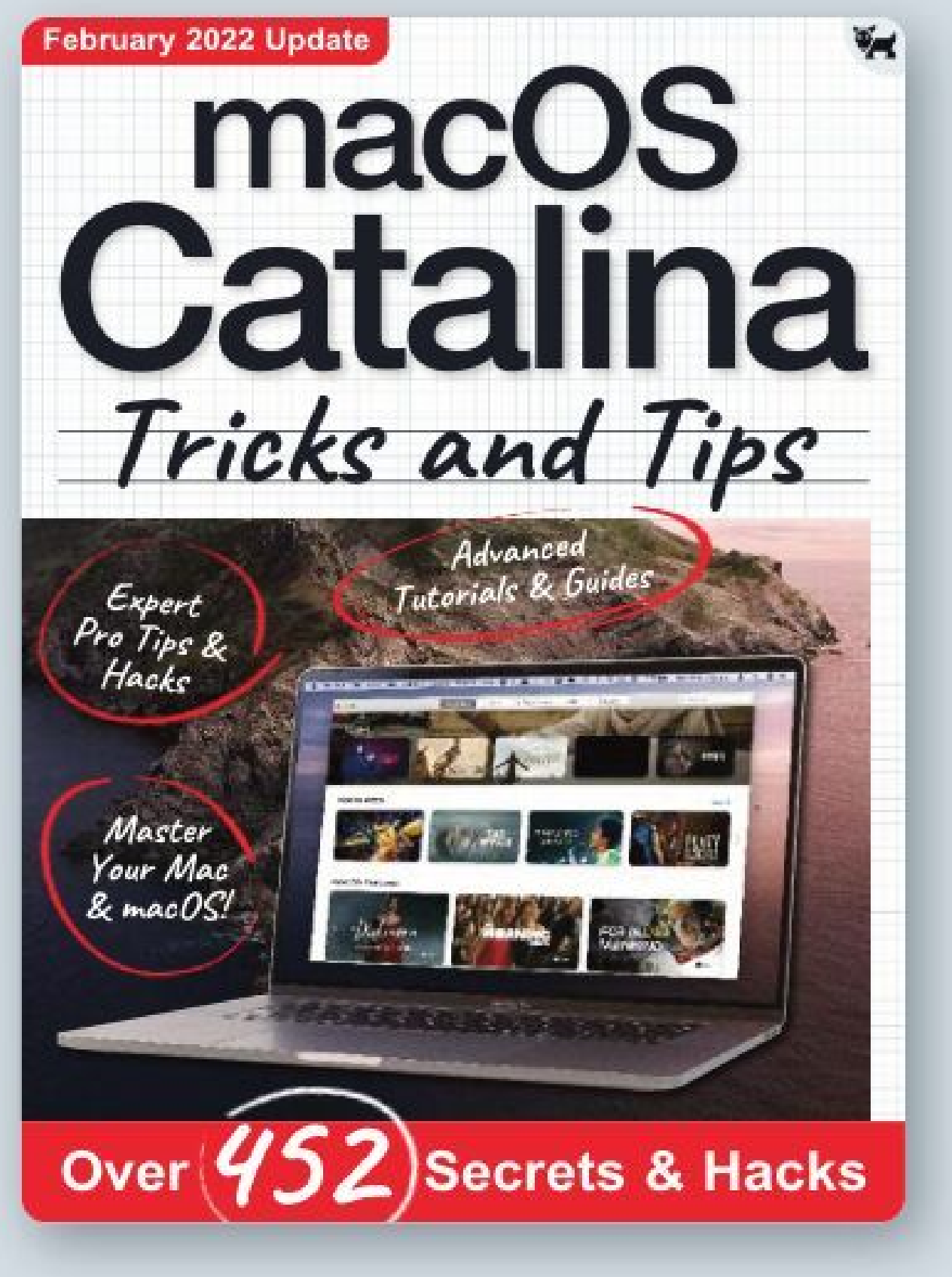

February 2022 Update
Coding
Tricks and Tips
Over 452 Secrets & Hacks

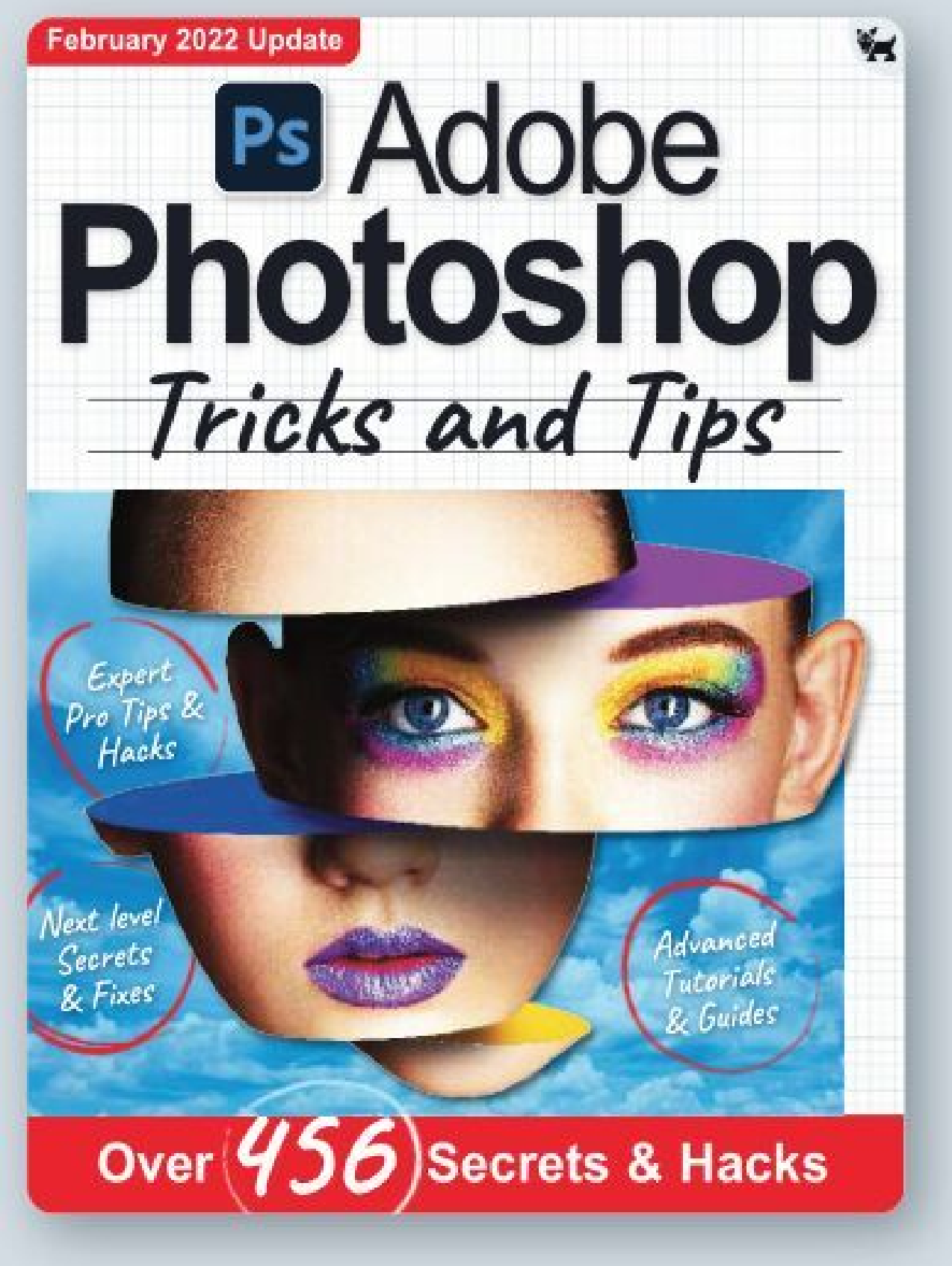
Tech Guides
Available on Readly

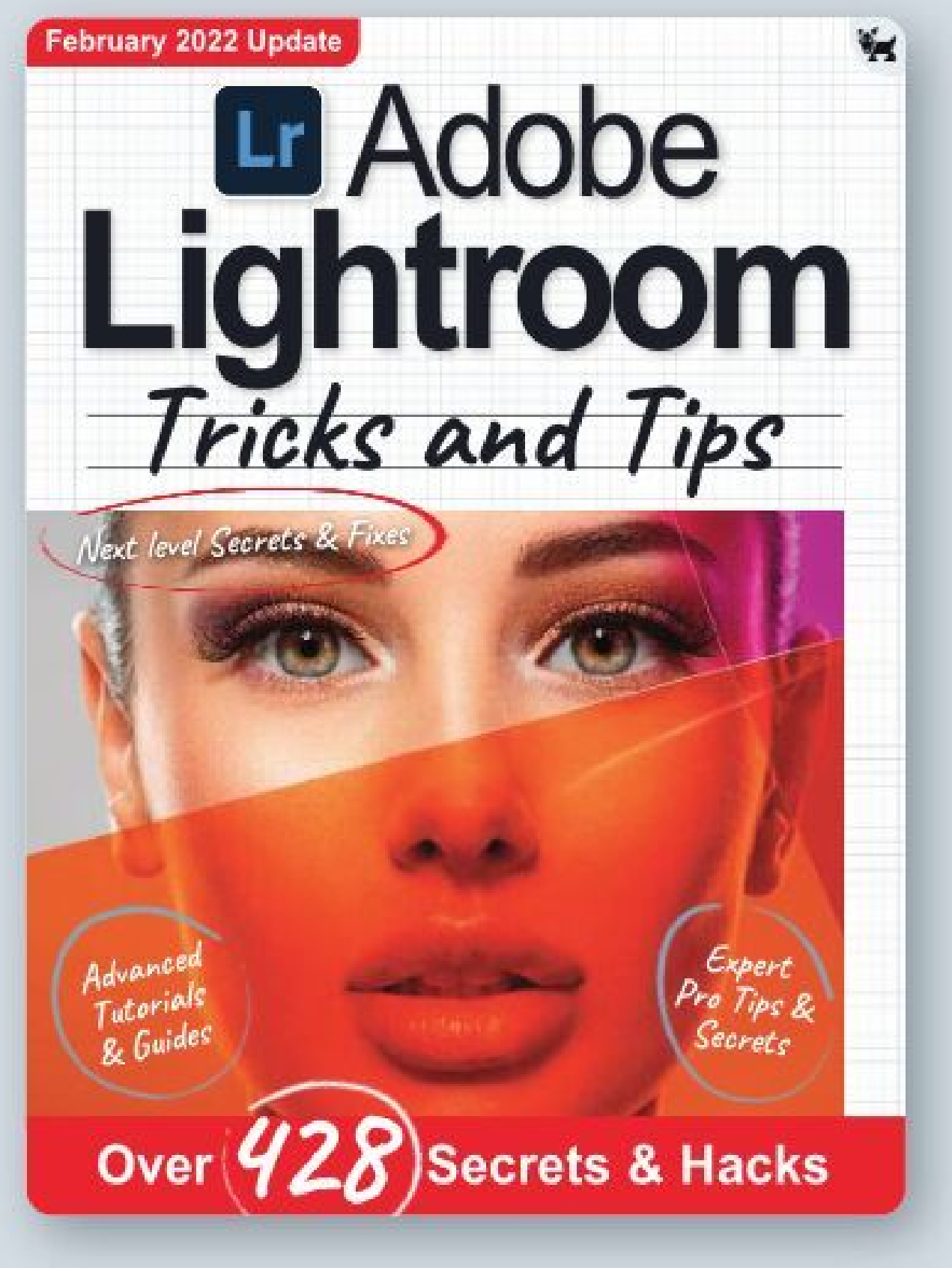

February 2022 Update
iOS 14
For iPhone & iPad
Tricks and Tips
Over 467 Secrets & Hacks

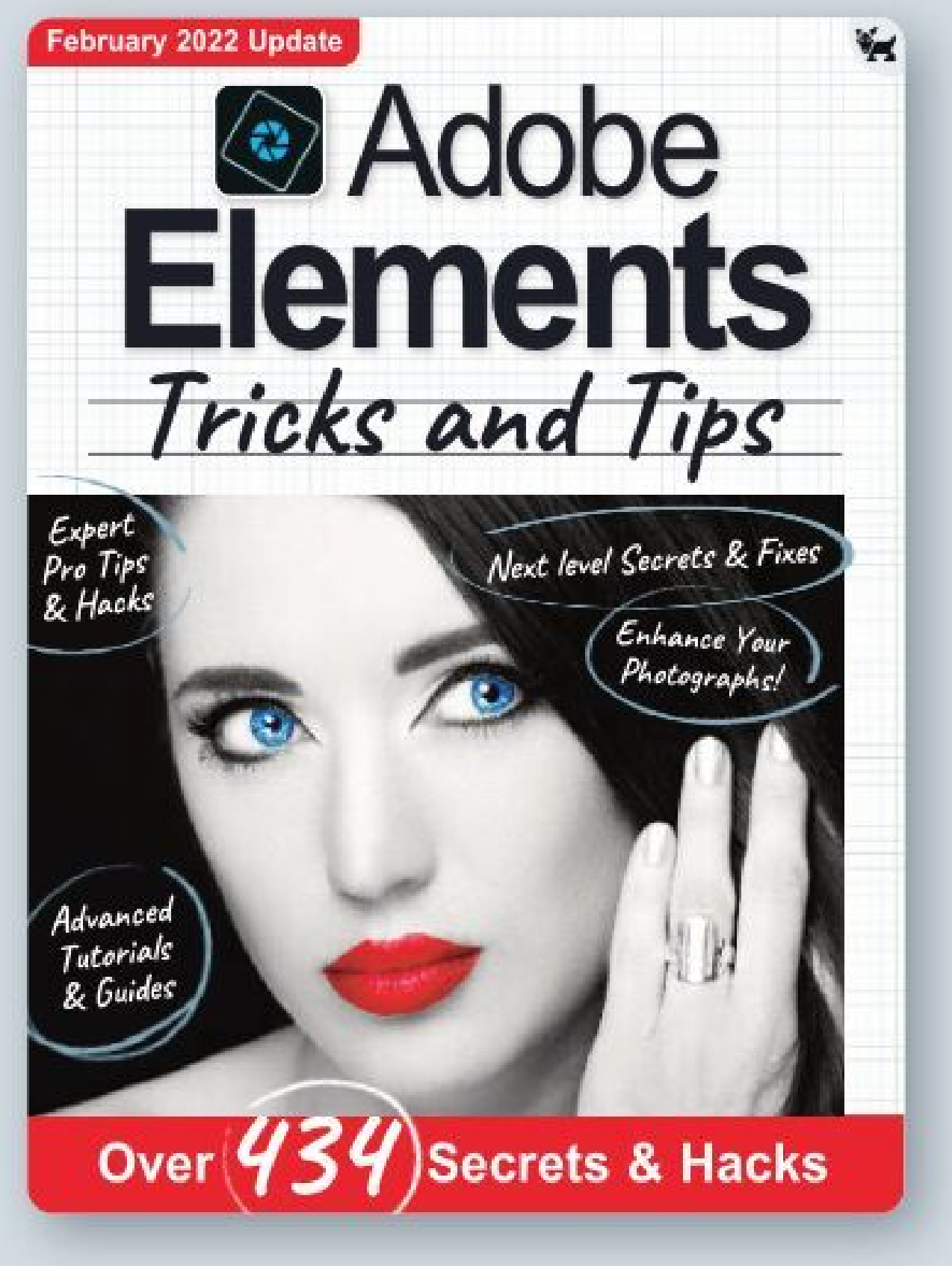

February 2022 Update
macOS Monterey
Tricks and Tips
Over 481 Secrets & Hacks

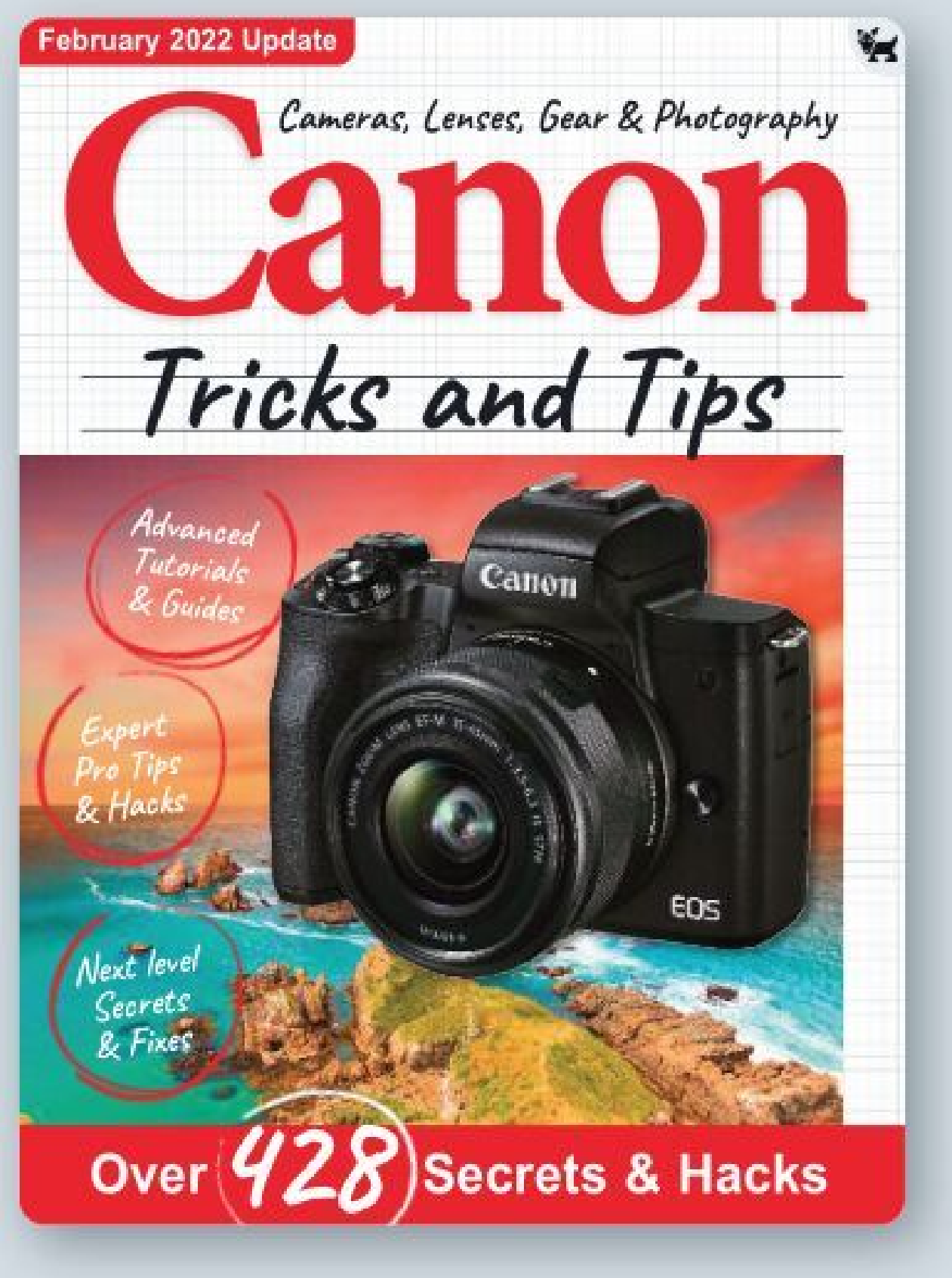

February 2022 Update
macOS Big Sur
Tricks and Tips
Over 449 Secrets & Hacks

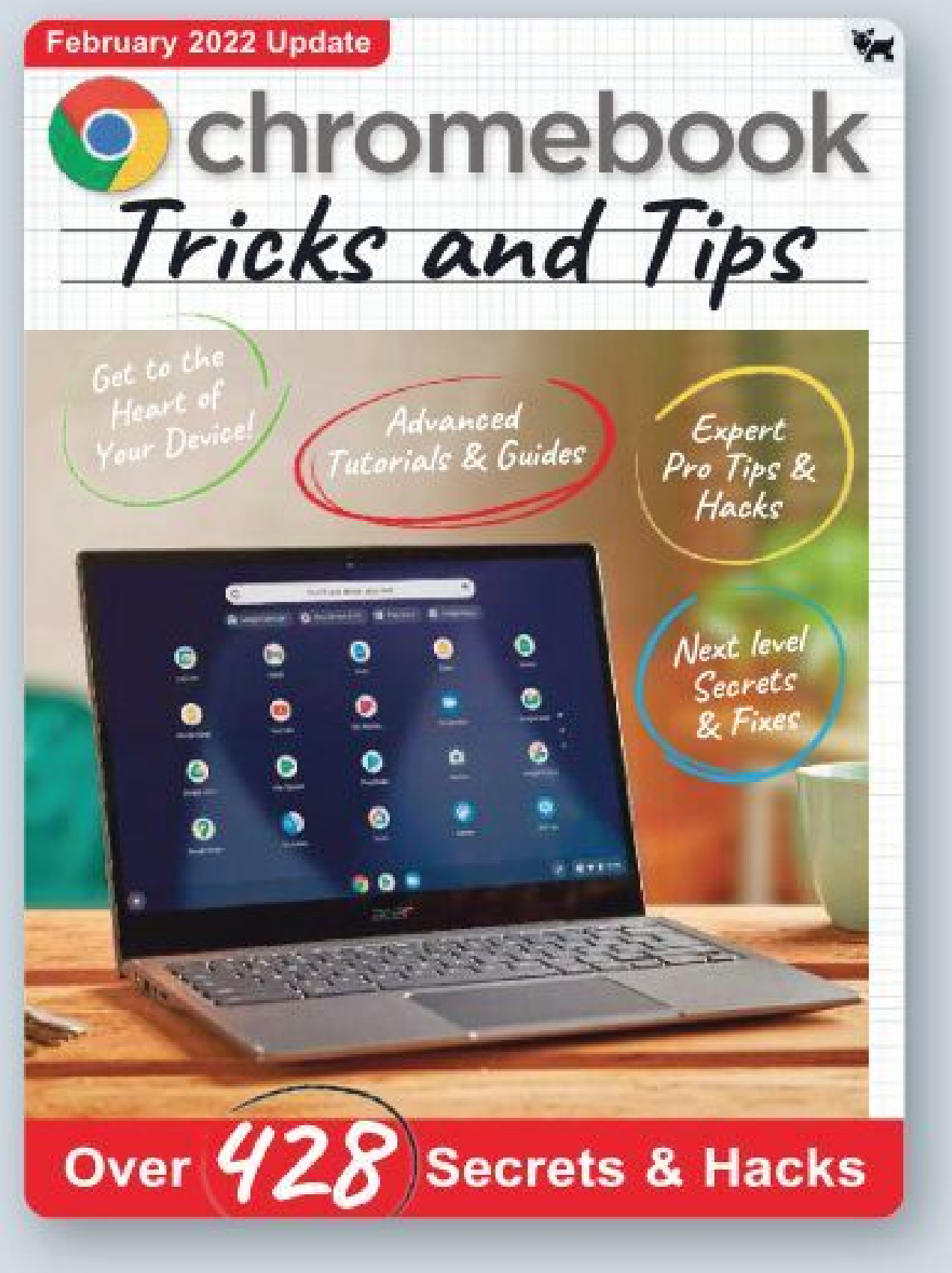

February 2022 Update
macOS Catalina
Tricks and Tips
Over 452 Secrets & Hacks

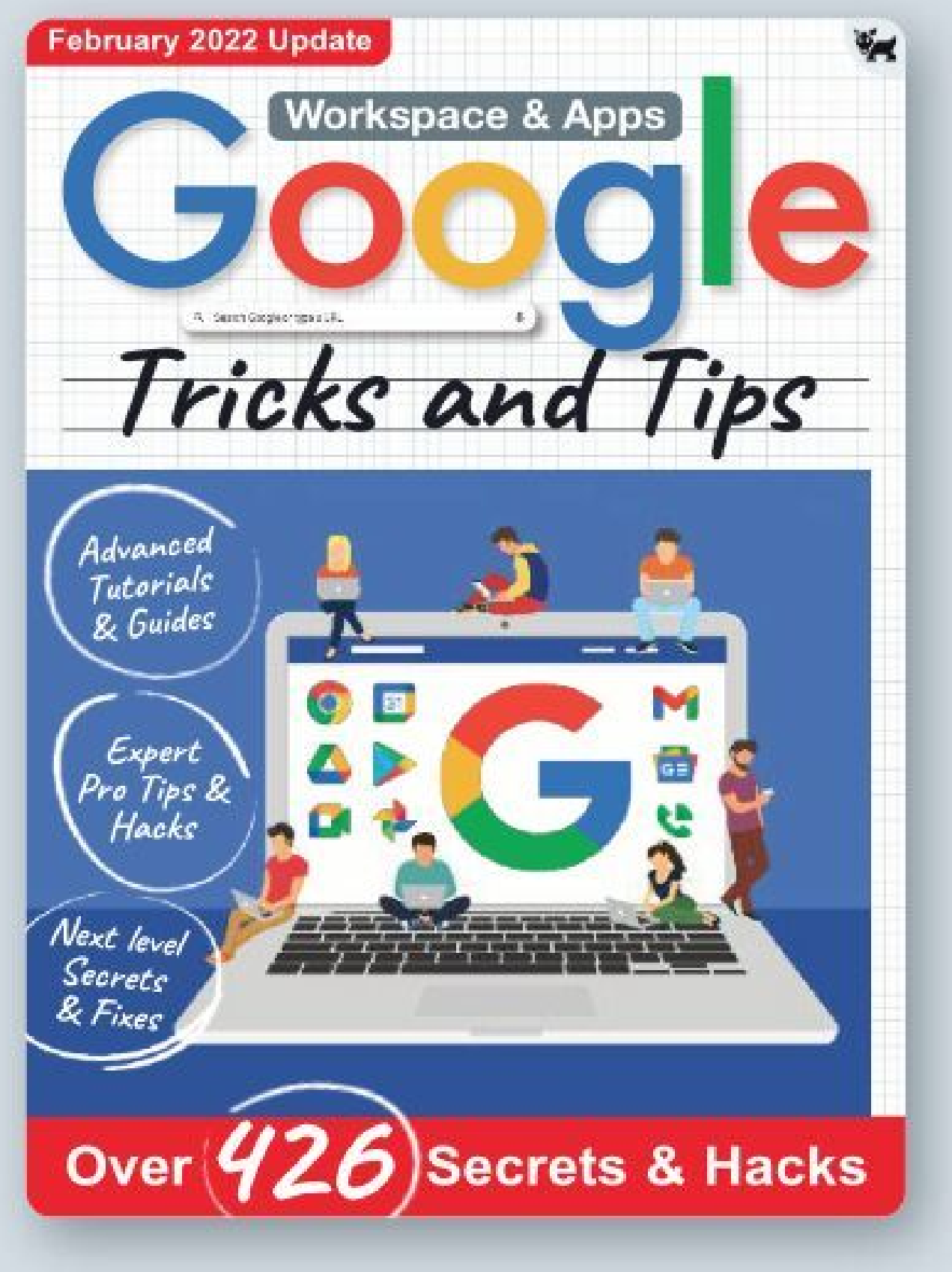

February 2022 Update
Adobe Photoshop
Tricks and Tips
Over 456 Secrets & Hacks

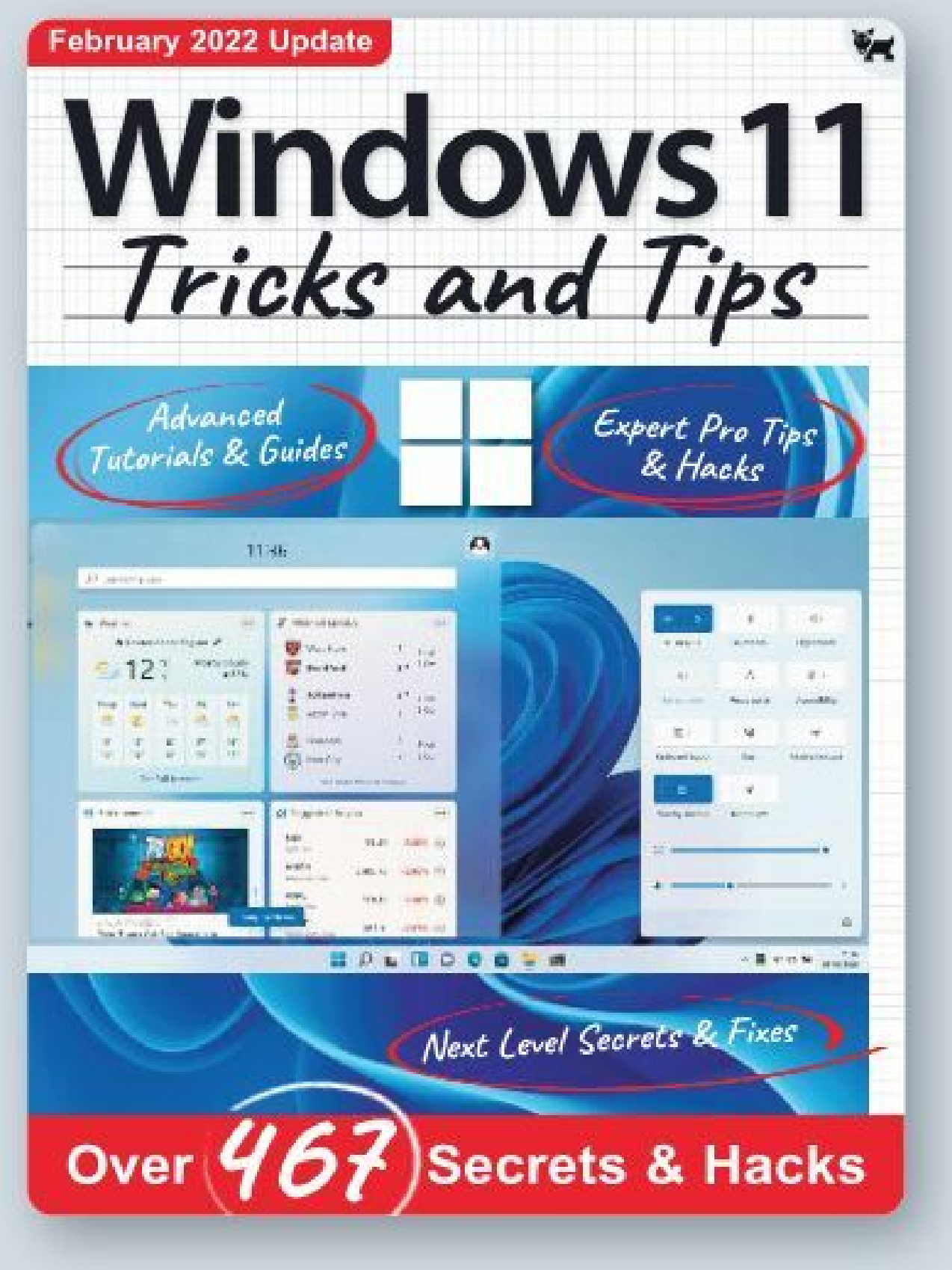

February 2022 Update
Adobe Lightroom
Tricks and Tips
Over 428 Secrets & Hacks

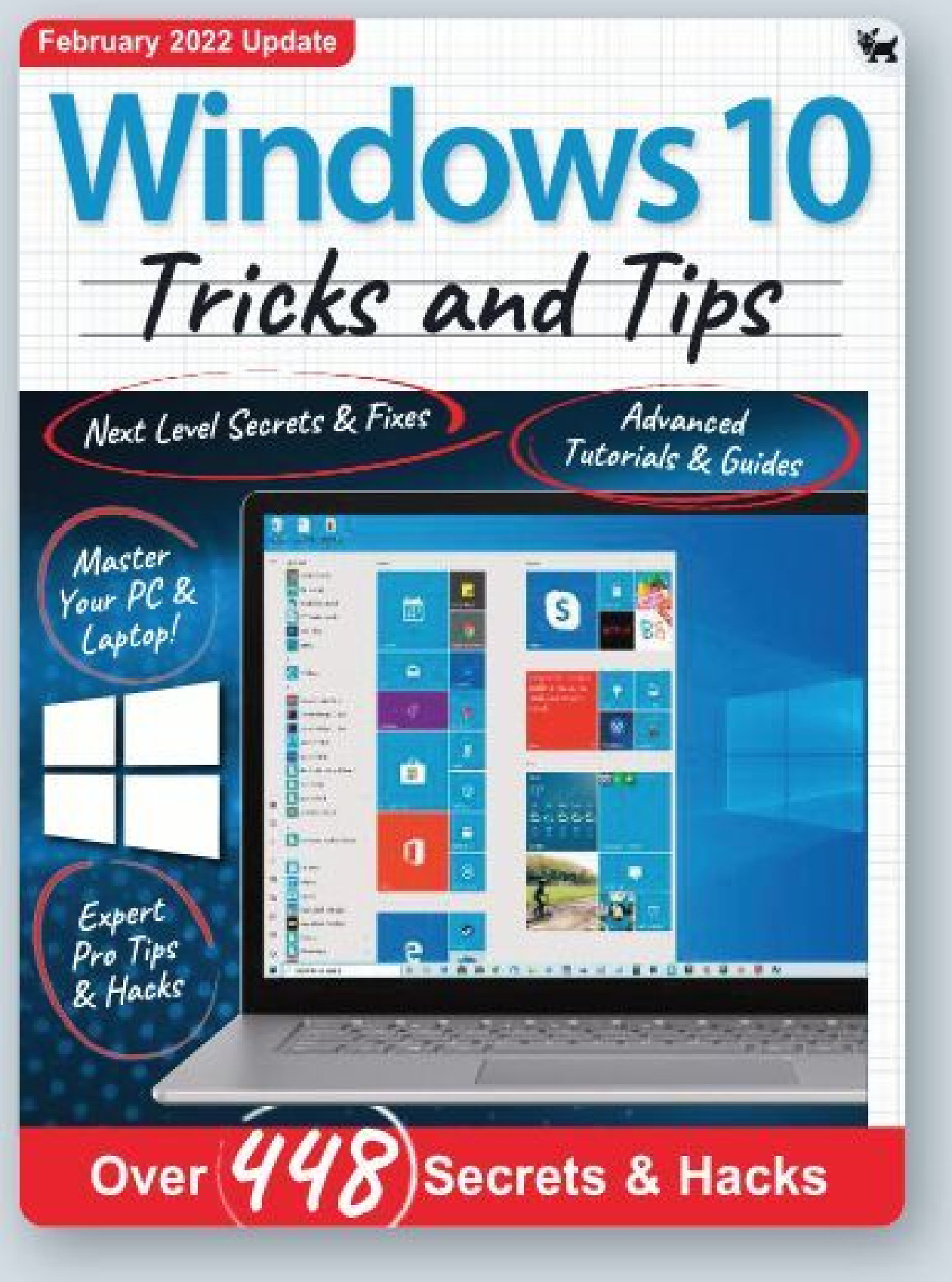

February 2022 Update
Adobe Elements
Tricks and Tips
Over 434 Secrets & Hacks

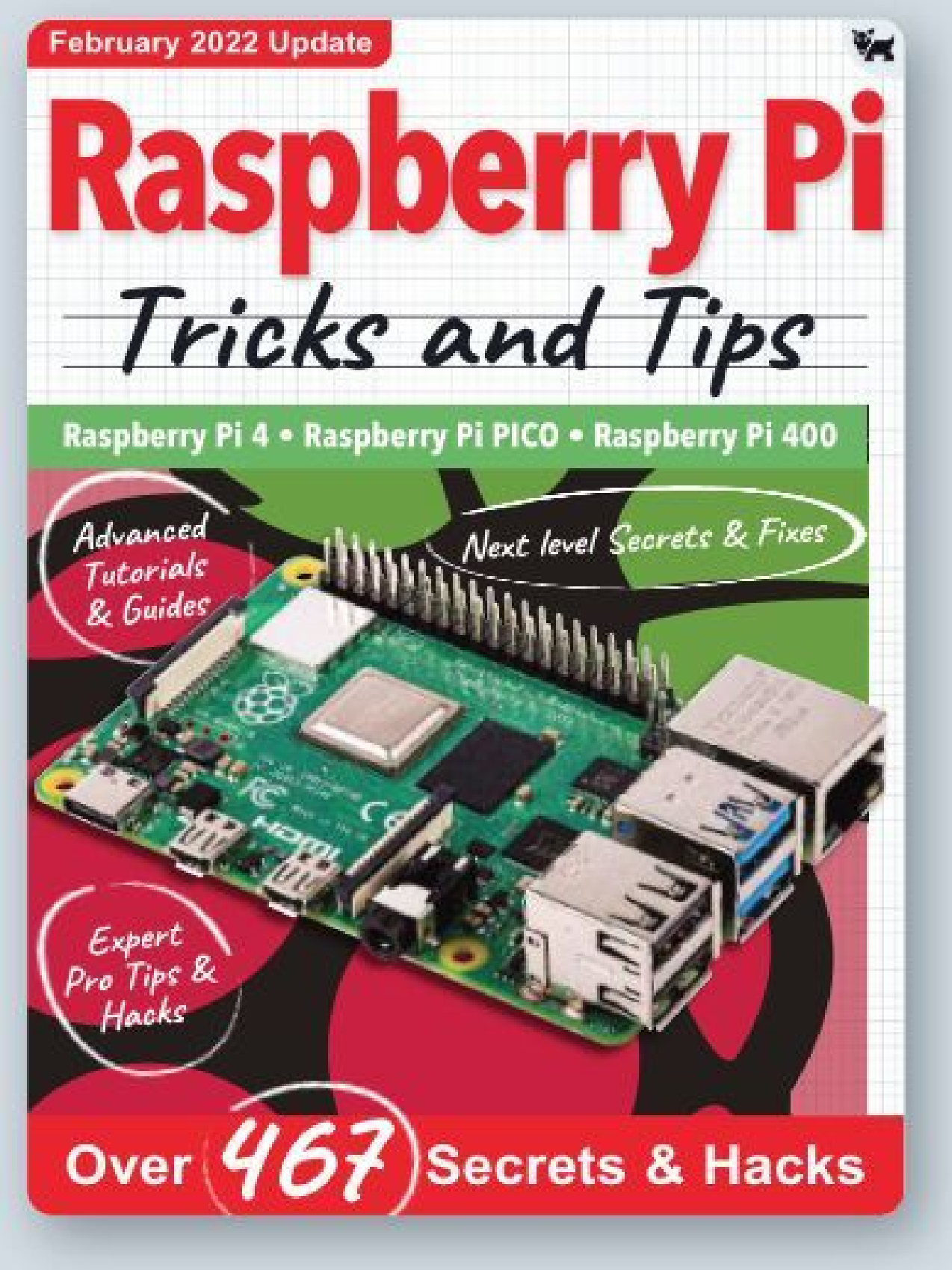

February 2022 Update
Cameras, Lenses, Gear & Photography
Canon
Tricks and Tips
Over 428 Secrets & Hacks

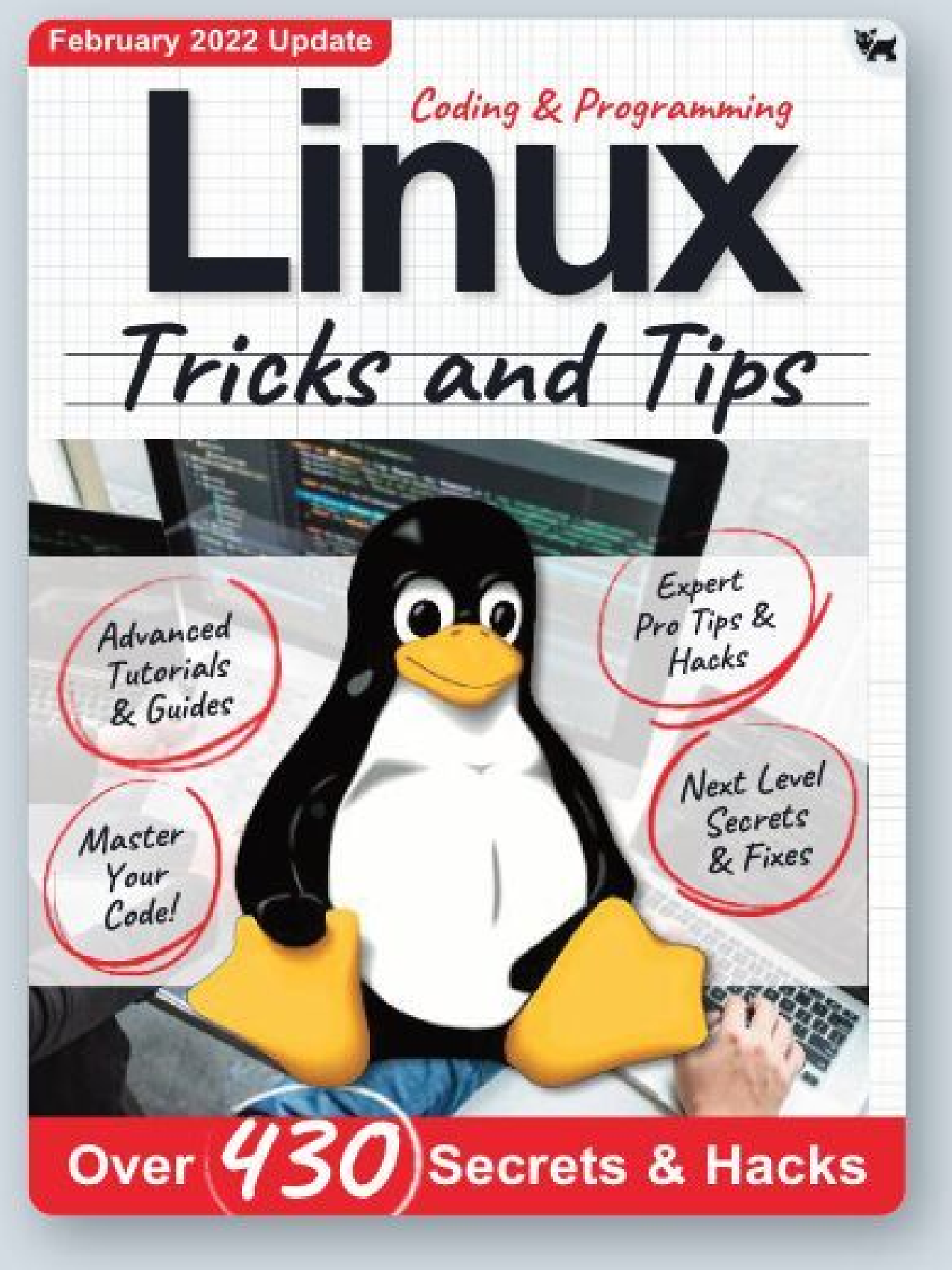

February 2022 Update
chromebook
Tricks and Tips
Over 428 Secrets & Hacks

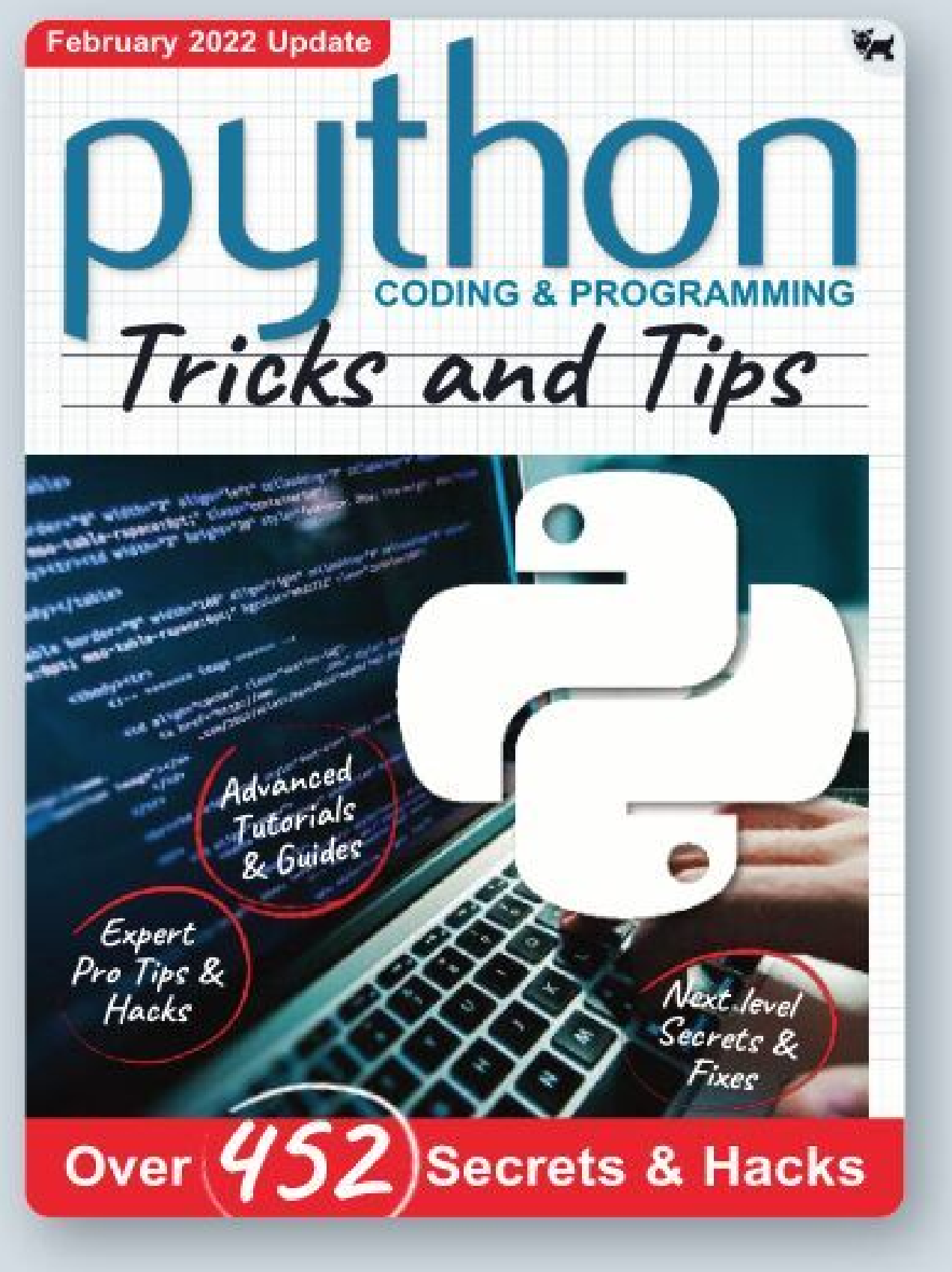

February 2022 Update
Workspace & Apps
Google
Tricks and Tips
Over 426 Secrets & Hacks

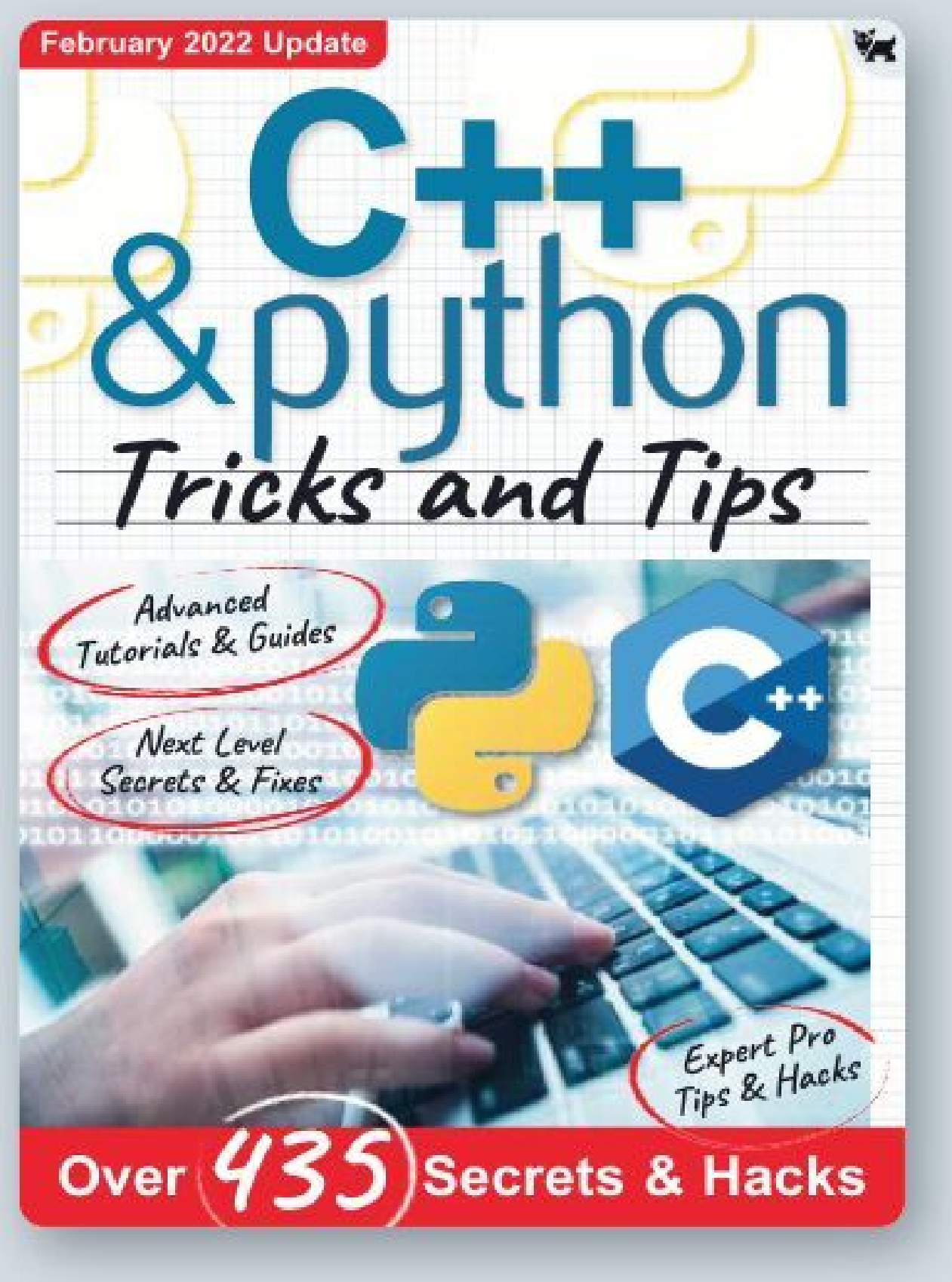

February 2022 Update
Windows 11
Tricks and Tips
Over 467 Secrets & Hacks


February 2022 Update
Windows 10
Tricks and Tips
Over 448 Secrets & Hacks


February 2022 Update
Raspberry Pi
Tricks and Tips
Raspberry Pi 4 • Raspberry Pi PICO • Raspberry Pi 400
Over 467 Secrets & Hacks


February 2022 Update
Coding & Programming
Linux
Tricks and Tips
Over 430 Secrets & Hacks


February 2022 Update
python
CODING & PROGRAMMING
Tricks and Tips
Over 452 Secrets & Hacks


February 2022 Update
C++ & python
Tricks and Tips
Over 435 Secrets & Hacks

www.bdmpublications.com

Congratulations, we have reached the end of your latest tech adventure. With help from our team of tech experts, you have been able to answer all your questions, grow in confidence and ultimately master any issues you had. You can now proudly proclaim that you are getting the absolute best from your latest choice from the ever changing world of consumer technology and software.

So what's next? Do you want to start a new hobby? Are you looking to upgrade to a new device? Or simply looking to learn a new skill?

Whatever your plans we are here to help you. Just check our expansive range of **Tricks and Tips** & **For Beginners** guidebooks and we are positive you will find what you are looking for. This adventure with us may have ended, but that's not to say that your journey is over. Every new hardware or software update brings its new features and challenges, and of course you already know we are here to help. So we will look forward to seeing you again soon.

www.bdmpublications.com

Black Dog Media

Master Your Tech

FROM BEGINNER TO EXPERT

To continue learning more about Your Tech visit us at:

www.bdmpublications.com

FREE Tech Guides

Apple iPhone, iPad, Mac, MacBook & Watch

PC, Windows 11 & 10

Samsung & Google

Photography, Photoshop, Lightroom & Elements

Coding Python, C++, Raspberry Pi & Linux

EXCLUSIVE OFFERS & DISCOUNTS on Our Tech Guidebooks

- Print & Digital Editions
- Featuring the Latest Updates
- Step-by-step Tutorials & Guides
- Created by BDM Experts

The iOS 15 iPhone GuideBook
Coding for Beginners
Windows 11 The Essentials

BDM's
Ultimate Photoshop

bdmpublications.com/ultimate-photoshop

Buy our Photoshop guides and download tutorial images for free! *Simply sign up and get creative.*

PLUS SPECIAL DEALS and Bonus Content When you sign up to our monthly newsletter!

Online Security Tricks and Tips
9th Edition | ISBN: 978-1-912847-66-2

Published by: Papercut Limited
Digital distribution by: Readly, Pocketmags & Zinio

© 2022 Papercut Limited. All rights reserved. No part of this publication may be reproduced in any form, stored in a retrieval system or integrated into any other publication, database or commercial programs without the express written permission of the publisher. Under no circumstances should this publication and its contents be resold, loaned out or used in any form by way of trade without the publisher's written permission. While we pride ourselves on the quality of the information we provide, Papercut Limited reserves the right not to be held responsible for any mistakes or inaccuracies found within the text of this publication. Due to the nature of the tech industry, the publisher cannot guarantee that all apps and software will work on every version of device. It remains the purchaser's sole responsibility to determine the suitability of this book and its contents for whatever purpose. Any app, hardware or software images reproduced on the front cover are solely for design purposes and are not necessarily representative of content. We advise all potential buyers to check listings prior to purchase for confirmation of actual content.
All editorial herein is that of the reviewer - as an individual - and is not representative of the publisher or any of its affiliates. Therefore the publisher holds no responsibility in regard to editorial opinion or content. This is an independent publication and as such does not necessarily reflect the views or opinions of the producers of apps, software or products contained within. This publication is 100% unofficial and in no way associated with any other company, app developer, software developer or manufacturer. All copyrights, trademarks and registered trademarks for the respective companies are acknowledged. Relevant graphic imagery reproduced with courtesy of brands, apps, software and product manufacturers. Additional images are reproduced under licence from Shutterstock. Prices, international availability, ratings, titles and content are subject to change. Some content may have been previously published in other editions. All information was correct at time of publication.

Papercut Limited
Registered in England & Wales No: 04308513

INTERNATIONAL LICENSING
Papercut Limited has many great consumer tech, coding, photography and Photoshop image editing publications and all are available for licensing worldwide.
For more information email: james@bdmpublications.com